10-30-2020

A Novel Physical Unclonable Function (PUF) Featuring 0.113 FJ/B for IOT Devices

Harikrishnan Balagopal
University of Windsor

A NOVEL PHYSICAL UNCLONABLE FUNCTION (PUF) FEATURING 0.113 FJ/B FOR IOT DEVICES

by

Harikrishnan Balagopal

A Thesis
Submitted to the Faculty of Graduate Studies
through the Department of Electrical and Computer Engineering
in Partial Fulfillment of the Requirements for
the Degree of Master of Applied Science
at the University of Windsor

Windsor, Ontario, Canada

2020

A NOVEL PHYSICAL UNCLONABLE FUNCTION (PUF) FEATURING 0.113 fJ/b FOR IoT DEVICES

by

Harikrishnan Balagopal

APPROVED BY:

R. Riahi
Department of Mechanical, Automotive and Materials Engineering

B. Shahrrava
Department of Electrical and Computer Engineering

M. Mirhassani, Advisor
Department of Electrical and Computer Engineering

19 August, 2020

Declaration of Originality

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I declare that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owners to include such materials in my thesis.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

Abstract

A physically unclonable function (PUF) is useful for authentication purposes and is a function created for its inherent uniqueness and inability of adversaries to duplicate it. In this thesis, a PUF is designed, which is a combination of both digital and analog circuits. This PUF could be designed partially based on a semi-automated approach using custom-built P-cells.

The PUF is implemented using novel digital circuits, which have been designed using basic digital gates with a minimal number of transistors. The proposed PUF is developed by the introduction of a layer of multiplexers, which is triggered by a novel SR-latch based model for driving the selection lines. For a higher bit stability, the SR latch is combined with four-way asynchronous circuits, which are a class of coincident flip-flops.

The resulted PUF consumes very little power and is suitable for sensors and low power applications. The proposed design was implemented in using the Cadence virtuoso IC 5.1.4 and based on the 180nm TSMC transistor models.

The energy consumption and area of the proposed PUF is shown to be equal to 0.1132 fJ/bit and 8.03, which is considerably lower than the state of the arts. The uniqueness and reliability of the proposed PUF are estimated to be 48.66% and 99.33%.

Dedication

"Dream, dream, dream. Dreams transform into thoughts and thoughts result in action."

by Dr. APJ Abdul Kalam

Dedicated to my loving Parents Dr. Balagopal Balakrishna Pillai and Jayasree S; my sibling Gopikrishnan Balagopal; my grandparents Dr. Balakrishna Pillai and retired deputy collector Savathri S Nair; My mentor Dr. Raju Garudachar. Thank you for always being there and their love. Thank you for the indestructible wealth of all time. I would also like to thank my supervisor, Dr. Mitra Mirhassani for her guidance and support.

Acknowledgements

I would like to sincerely thank my supervisor, Dr. Mitra Mirhassani, for her guidance and support in successfully completing my thesis. I am deeply grateful for her involvement, guiding, mentoring and providing any help that I needed to complete my degree. It is an honor to have worked under her supervision.

I would also like to thank my committee members, Dr. Behnam Shahrrava, Dr. Arash Ahmadi and Dr. Reza Riahi for their encouragement, constructive comments and positive criticism which in fact, improved my ideas and solutions.

I would like to extend my gratitude to my colleagues at the Analog Mixed signal research labs (AMS-labs). I appreciate their friendship, support, encouragement, their constant involvement and valuable feedbacks. Finally, I would like to thank the research received from Canadian Microelectronics Corporation (CMC) Microsystems.

Table of Contents

List of Tables

List of Figures

List of Acronyms

GMM	Gaussian Mixture Model
NP	Noise Perturbation

Chapter 1

Introduction

Internet of things (IoT) is becoming pervasive in today's world. Approximately 31 billion IoT devices are made by 2020. These devices are extending connectivity beyond standard devices such as desktops, smartphones, and other electronic devices, to any range of nonelectronic physical devices and everyday objects. These electronic devices are embedded with technology that could make the device self-working, i.e., interacting over the internet and even remotely controlled and monitored. The widespread usage of these devices, several challenges hinder a successful deployment of an IoT system. Parameters such as security, interoperability, power/processing capabilities, scalability, and availability must be considered. There is a rapid concern for security in devices when software rules the majority of the control.

1.1 Motivation

Reducing the power utilization is one of the essential plan objectives for many mixed-signal circuits, frameworks, and applications, for example, cell phones and high-performance computing systems. Hardware-level protection for circuits without the usage of software started a decade back promising security. The primary concern for these techniques was that these were extensively expensive in terms of cost, area, and power. Few commercial products were developed during the time including the IBM's 4758 tamper-proof packages, which was used to protect processors and other major units.

Intel and Atmel also brought their trusted platform module (TPM), which was a

specific hardware security unit. These two models had major disadvantages due to their cost of 3000 dollars for a 99MHz processor and 128MB of memory for IBM4758 while Intel and Atmel's TPM were hacked by experts and proved that the decrypted secondary keys could be read out from the bus [12]

Physical unclonable functions (PUF) are one of the most promising security solutions used for authentication and secret key storage, meanwhile storing no information in host devices. Each host device is fabricated and is induced with natural process variations which could be slightly different from their ideal values. PUF takes advantage of the manufacturing imperfection to create a secure authentication signature for the device. Since no two devices can be fabricated exactly the same, a PUF is created using these differences for the generation of a unique signature for each device. The value of the PUF cannot be predicted even by the manufacturing facility, since these imperfections are random.

1.2 Market assessment

IoT devices trend and rapid growth were belligerently watched by the tech world during the past years. According to a survey by Gartner in 2017 [13], the IoT devices were in use to reach 8.4 billion, which is an increase of 32% over the past year.
Also, the estimations for the future development of IoT gadgets have been quick and irate. At the high end of the scale, Intel anticipated web empowered gadgets to increase from 2 billion in 2006 to more than 200 billion by 2020. This means that each person has approximately 26 smart devices.
Somewhat more preservationist, IHS Markit [13] said the number of associated gadgets would be 75.4 billion of every 2025. Additionally, the social insurance industry is likewise defenseless against these assaults as IoT therapeutic gadgets associated with the system have low versatility to digital assaults. Medical gadgets and embeds, such as cardiovascular pacemakers and imbuement siphons, can affect well-being whenever

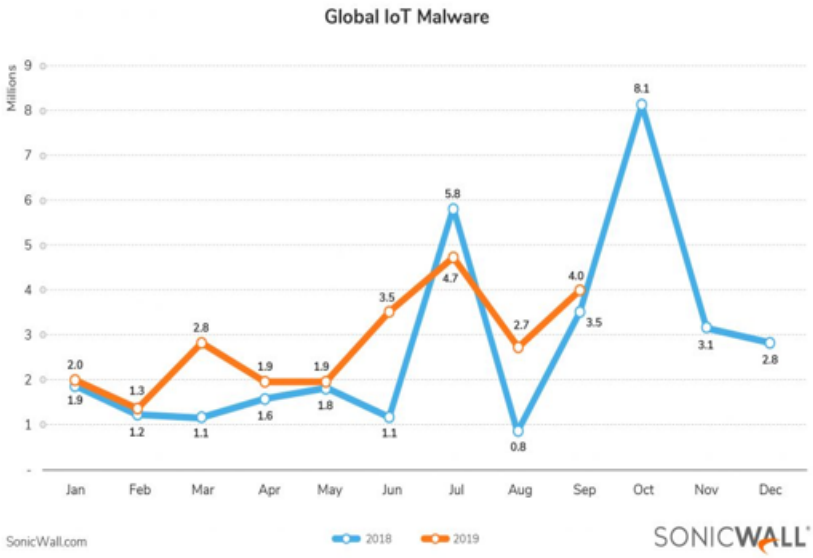

Figure 1.1: Market assessment

[14]

the programmers alter it. The danger of digital assaults is with the end goal that it can upset the working of a medical clinic by obliterating the whole data innovation framework. These are some of the recent cyber-attacks reported. It is estimated that the end of this decade could triple cyber attacks. Countering the cyberattacks, researchers have developed a highly classified technology in terms of software level, which could act as a wall for these attacks. Researchers switched their attention towards the hardware level of security as the scope of exploration towards has significantly proved the capacity of these days.

1.3 Physical Unclonable Functions

A physical unclonable function (PUF) is a device that utilizes inbuilt randomness introduced during fabrication which creates a unique digital signature or fingerprint. The main problem with these types of protection is that the secret key has to be

stored in the in non-volatile memory.

These highly sensitive data could be retrieved using invasive attacks. PUF is a challenge-response primitive used in a physical system to provide the required security measures instead of storing the secret key in memory. A PUF generates a response to a given challenge. The idea behind the PUF is that the output response is random and unpredictable. moreover, the response of two PUFS to the same challenge is different.

This is because the PUF response depends solely on the unique and random characteristics of physical devices, such as gate delays. The very important feature of a PUF is its unclonability, i.e., even if an attacker has access to the circuit and builds the same circuit using the same technology, its response to the given challenge would be different from that of the first device.

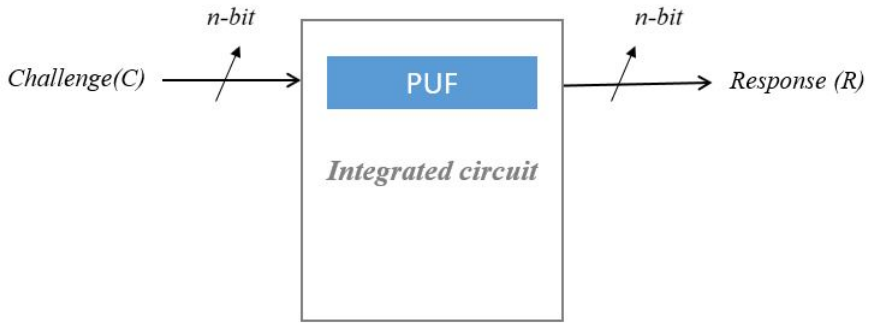

Figure 1.2: General overview

Physical unclonable function (PUF) could serve as a fundamental building block for any system that communicates. PUF has gained a lot of attention both in terms of research and industrial. The primary goal for creating such a circuit is securing applications like intellectual property, hardware privacy, authentication. An ideal PUF unit would be a circuit that produces a random set of responses for n number of challenges. The responses made should be unique for each unit made and should be unclonable.

All PUF models exiting today suffer from substantial limitations such as poor efficiency, bit stability, reliability, and uniqueness. Out of all these parameters, power consumption is a very notifiable parameter. Less power consumption in devices such as IoT devices helps us covering issues like efficiency. This work presents a substantial improvement in the creation of better PUF units by introducing the concept of multi-level randomness. Almost all PUFs suffer from a limited number of challenge-response pairs, Bit-Error Rate (BER) as well as the effect of temperature.[15].

1.3.1 PUF Architecture

There are various methods for constructing a PUF. Non-electrical PUFs include Optical PUFs [16], Acoustical PUFs and Coating PUFs. Optical PUFs use an optical micro-structure which is built by mixing microscopic refractive glass spheres on a tiny transparent epoxy plate while Acoustical PUFs are built upon by using acoustical delay lines. In Coating PUFs, a protective coating material is inserted onto the device using random dielectric particles that have random properties in size, shape, and location.

However; these devices are extensively costly to build. On the other hand, there are various silicon-based PUF models [17] are such as Memory-based, Glitch-based, Delay-based PUF. Memory-based PUFs include SRAM, SR Latch, Flip-Flop, Butterfly, and Bus keeper PUFs. These works are based on metastability, which produces randomness in them. While delay-based PUFs consists of Arbiter PUFs, Ring-Oscillator PUFs (RO PUFs), and Glitch PUFs [15].

1.3.2 PUF Ideal Properties and Features

The properties of PUF are as follows, reliability, uniqueness, uniformity, and bit-aliasing.

Reliability is indicated how a PUF can reproduce its outputs with respect to time as

well as a varying condition such as, under factors such as environmental conditions and aging the device keeps its performance stable and reproduce the same quality of result which was produced before.

The ideal value of reliability is 100% [15]. Uniqueness is a measure of inter-distance variations of the response bits among different PUF instances. In other words, if a specific challenge is applied to two identical PUF instances, the response of the two PUFs should be different. Ideally, this value should be 50%. Uniformity of an ideal PUF is 50% meaning that 50% of the response, bits are one, and 50% are 0, and therefore, the PUF the response does not have a biased behavior towards a specific bit value.

Another important factor of a PUF, which also represents the randomness of the PUF response is bit-aliasing. Bit-aliasing of a given bit position in the PUF response is its percentage Hamming Weight (HW) across several PUF instances [18] [19]. Again, this value should be ideally 50% for all response bit positions.

1.3.3 PUF Applications

The primary reason for the development of PUF units is for applications such as authentication and secret key generation.

Authentication is performed in two steps [15]. The implementation of authentication takes place in the enrolment phase and verification phase. To begin with, in enrolment phase various challenge-response pairs(CRPs) is recorded(noted/ Stored) by authentication(Validation) authority in a database. After this, in the verification phase(stage), an arbitrary challenge is picked from the data and applied to the PUF under verification. If the stored and generated response is significantly close, the PUF is validated.

The authentication system can be attacked (raid) by a hacker(attacker) as the CRP, which is chosen by the authentication party is communicated(moved) over an unreliable channel. Therefore, to reduce(avert) such an attack, CRP should be uti-

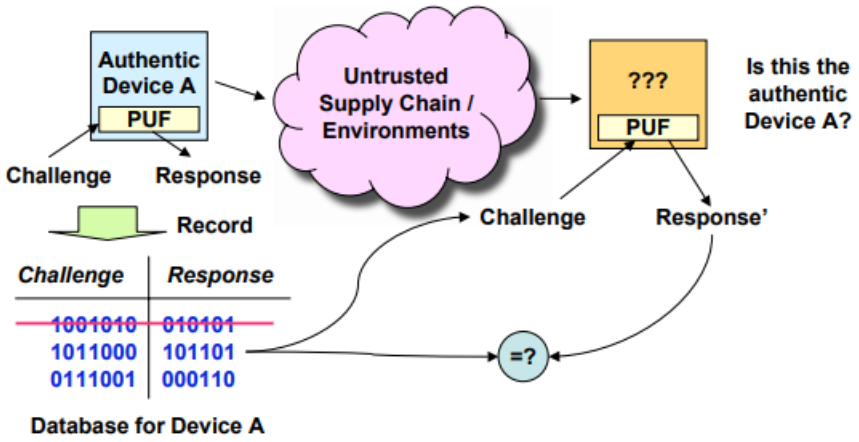

Figure 1.3: Overview of PUF-based authentication

[2]

lized only once during the authentication process. Hence, PUF should produce enormous CRP to authenticate(verify) devices multiple times before CRP is exhausted.

Therefore, the utilized PUF should provide a large number of challenge-response pairs so that a device can be authenticated as many times as required before the CRP set is exhausted.

However, in a secret key generation, an inexhaustible(unlimited) particular key needs to be generated. There is no secret key in the system, but the PUF circuit creates it at the time of requirement. Similarly, in the reconstruction phase for storing key PUF need to create an unlimited response; and if the response is the same as the stored key, the response is recognized as a valid key. The focal point(focus) of the thesis is to create a PUF circuit for generating a huge number of responses.

In the reconstruction phase for the key storage process, the same challenge is applied to the PUF. If the response if the same as the stored key, the repones is recognized as a valid key.

it should be noted that the focus of the thesis is to implement a PUF, which is able to generate a large number of responses. It is the goal of this research to increase

the bit-length and randomness of the PUF to reduce the probability of estimation or guesses of the output bit. The security of the server and issues related to the communication link between the PUF and server are outside the focus of this research and should be considered in separate research.

1.4 Thesis outline

This thesis is organized in the following chapters as follows:

Chapter 2: Literature Survey

In this chapter, a literature review is conducted on multiple styles of PUF implementation such as analog, digital, and mixed-signal PUFs. Among various types of PUFs, ten of the more competitive PUF models, as the state of art development were studied in more detail. Selected ones are implemented in cadence virtuoso IC 5.1.4 on 180nm TSMC foundry. Literature study comparisons are made in this chapter.

Chapter 3: Implementation of PUF models

The proposed PUF is designed using the provided models by the Canadian Microelectronics Corporation, and in TSMC $180nm$ technology node. The PUF was simulated using the Cadence Virtuoso IC 5.1.4 software. To ensure the eventual design robustness and evaluate its performance several Monte Carlo analysis was performed using the Specter models.

Chapter 5: Design details and Sub-Circuits

In this chapter, the design and implementation of the PUF are provided. The PUF structure and transistor model of the gates are presented in detail. This chapter also includes a novel proposed circuit for the SR latch and its future impact and development. Full design techniques and implementations are provided in this chapter.

Chapter 6: Conclusion

This chapter summarizes the results and presents potential area of research for future work.

Chapter 2

Literature Survey

This chapter describes how PUF works and briefly conducts a literature survey on different implementation styles of PUF.

Also, various styles of PUF models including delay-based, memory-based, and glitch-based are presented. Moreover, details of a few state-of-the-art PUF structures and designs are provided, and each one is classified for its advantages and disadvantages.

2.1 General Working Principle of a PUF

PUFs are mostly connected to sensors and actuators and are expected to work 24×7 and are in some instances are unmanned. The sensors within an IoT network are constantly communicating with the network, and are the most vulnerable points in a sensor network system. Therefore it is required to ensure their security, and be able to efficiently authenticate their operation in the network. Fig. 2.1 represents a general working model of a PUF unit.

A typical way of storing the keys for authentication purposes is to store their value on the device itself. In this approach when the sensor contacts the server, it uses the internal memory mechanism to produce the key required for authentication of the device. For this purpose, many devices are using regular encryption algorithms. It should be noted that this point in operation is when the device can get manipulated to reveal the secret key by using methods such as side-channel attacks. Therefore, an approach that does not depend on regularly creating the keys and hence requiring to

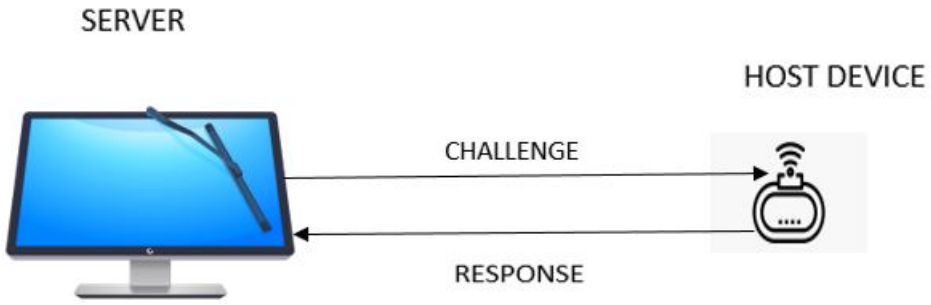

Figure 2.1: General working model

perform certain routine operations is more secure.

The PUF mechanism is based on only mechanical imperfection of the device to create electronic signatures. Here no keys are stored in any host devices and do not require to constantly read and transfer key values form the storage portion of the device to processing, and therefore are immune against side-channel attacks that rely on data transfer. Each device is distinguished based on their inherent mechanical randomness, i.e., each device produces unique keys which are challenge-response pairs. The keys are then extracted by a third-party vendor and are placed in a server, this technique is called bootstrapping: At manufacture, the server builds a database of CRPs for each device. At deployment, the server picks a random challenge from the database, queries the device, and validates the response [20].

Device authentication is an important application that should be considered when designing a PUF unit. Authentication primarily depends upon uniqueness and reliability. When a PUF device tries to authenticate the server verifies its CRPs with the host device. Fig. 2.2 demonstrates the authentication process [21]. If the same n-bit challenge is sent to several similarly constructed PUFs, it is expected to have different and unique responses from each. As a note, a larger bit-length response can authenticate a larger population of PUF units [2].

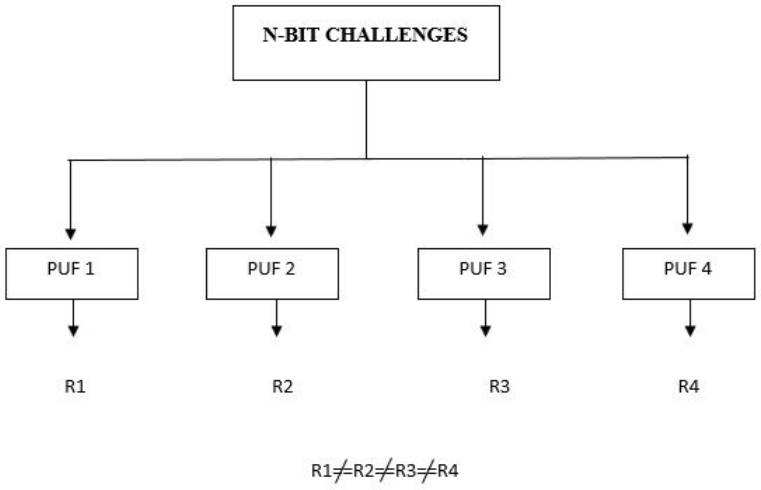

Figure 2.2: uniqueness for devices

2.2 Classifications of PUF

The unique construction of a PUF is set by the fabrication mismatch and manufacturing process. Minor natural variations in the nanoscale fabrication process are used to create the PUF signature. The physical unclonable function is considered as a black box for modern-day high-security applications.

These are broadly classified based on fabrication and security strengths describe the classification of PUF [15, 22].

2.2.1 Classification of PUF Based on Security

This division is based on the number of challenge-response pairs (CRPs) that could be generated using a PUF. This classification also depends on the quality of the responses obtained in association with the parameters.

The division of the PUF based on security create three main categories. Table 2.1 summarises the PUF division.

No.	Type (Security)	Feautres	Applications
1.	Weak PUF [23, 24] [25, 15]	1. Less vulnerability of getting cloned. 2. Responses are unpredictable and rely on the manufacturing variability of the device. 3. It is impossible to fabricate two devices with the equivalent digital signature. 4. A small number of CRPs (Challenge-response pair) 5. Access-restricted responses.	1. Used for low security application such as key storage (SRAM-PUF)
2.	Strong PUF [26, 27] [15]	1. Responses are highly stable to random readings of environmental conditions. 2. Unpredictability. 3. A large number of CRPs such that it takes much more time to enumerate the CRPs. 4. Power disspation is comparatively higher. 5. As in general more components stands for area.	1. Used for high security applications such as authentication
3.	Controlled PUF [28]	1. Combination of Strong PUF and a control logic unit.	1. High security applications (PUF-FSM)

Table 2.1: Classification of PUF based on security

Weak PUFs

This model has very few challenge-response pairs and is used in low-security applications such as RFID tags [23, 24]. They are mainly used to derive key in cryptographic algorithms and less vulnerable to modeling attacks [25].

Strong PUFs

This class operates with a large number of challenge-response pairs (CPRs) and usually operates in a higher frequency spectrum. This type of PUF is mostly used for device authentication purposes [27]. Generating unique CRPs on a large scale is always a challenge considering reliability and other device parameters. As the device operates in a high-frequency spectrum, even a small change and imperfection could lose a lot of CRPs [26].

Controlled PUF

This class of PUF is similar to that of a strong PUF, which has a very large number of challenge-response pairs while including a protected by the control logic. The CPRs are preprocessed, and then a logic unit wraps it with a protective algorithm before exposing it to the outside world. These types of PUF are mainly used in high-security applications, including critical authentication for devices. A controlled PUF is always fabricated, including the algorithm, so the PUF and algorithm are indivisible [15] [28].

2.2.2 Based on fabrication

This classification is simply based on the type of materials used to fabricate PUF units. As a note, the primary purpose of the PUF is increasing the strength of the authentication process and its security [15]. Fabricating PUF units inside the IC is always safer, more resistant to various types of attacks and are categorized as follows:

Silicon PUF

These are the most common type of PUF seen around. These are extremely cheap to built as they utilize a small part of the IC and are highly secured. The challenges for these IC are simply the inbuilt gate delays and other variations that are formed during its fabrication [15, 23].

Non- silicon PUF

These are mainly used for high-security applications, which involve a very large number of challenge-response pairs and are extremely costly to build.

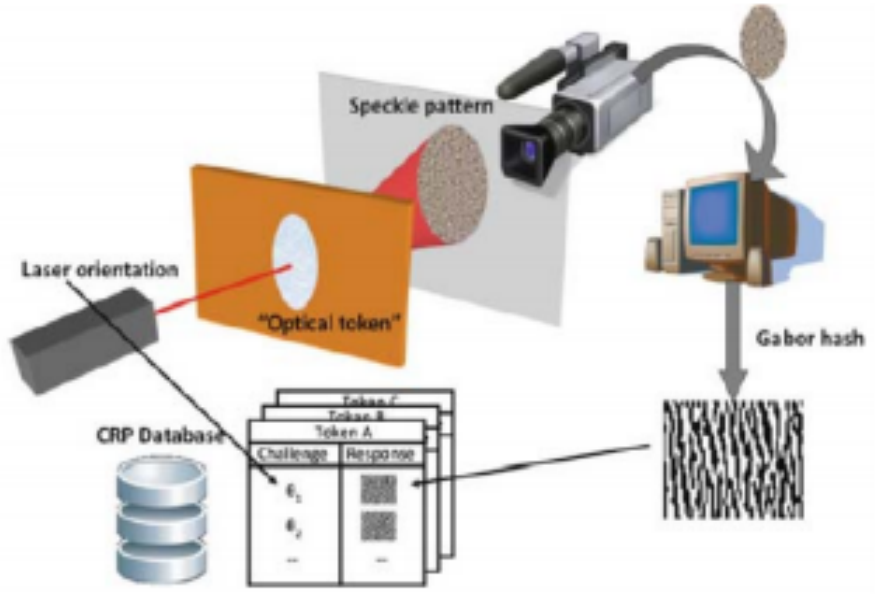

Figure 2.3: Basic implementation of an optical PUF [1]

The units are made separate from that of the actual IC and are more vulnerable to physical attacks. Some of the common examples include optical PUF, Acoustic PUF, coating PUF [29, 1]. Figure 2.3 shows a system which operates based on the optical PUF.

2.3 Delay based PUF

This type of PUF makes use of random variations in the delay of wires and gates. As in general a race condition is being set-up in the circuit, and it compares the two signals that propagate through the different wire to decide which reaches first. This section describes different types of delay models existing some include arbiter PUF, Ring oscillator PUF, Analog PUF, and Glitch PUF.

2.3.1 Arbiter PUF

Fig. 2.4 shown below represents an arbiter PUF. Several multiplexers are used in parallel is to exploit the propagation delay in each chain-like circuits. Each multiplexer is triggered by a selection line, which in turn controls the flow of the input signal to the next stage. Among the delay-based PUFs, Arbiter PUF [30] is the most used model due to its simplicity.

The basic concept is to let rising-edge signal travel through two different delay paths. At the end of the chain, an arbiter decides on the winning signal [31, 32]. This decision is made by a phase detector or a simple latch.

The multiplexers are designed in such a fashion that if the selection line is zero, the MUX Crisscross the chain else visa versa. Each selection line could be considered as a challenge given to the chain. The number of MUXs depends on the number of challenges given [8].

The design operation depends on various physical and manufacturing variations, i.e., the delay lines should be perfectly symmetrical to have an equal delay. As far as the arbiter PUF is considered, the design should be strong in such a way that it shouldn't produce various outputs for the same bits in different conditions.

There could be a scenario were the delay lines delay could be almost the same; at the time of this occurrence, the arbiter could enter a "metastable state". This state could induce the whole randomness into the circuit. This happens once the circuit

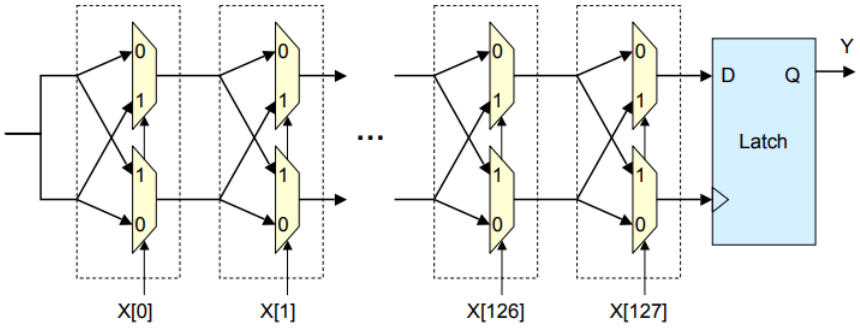

Figure 2.4: Arbiter PUF [2]

completely settles down to its original state, and this could be stated as unreliable as it could not be static for each device.

Implementation of this device was conducted in [33] using an FPGA platform; the drawback of asymmetric implementation model is that the routing of these delay lines is a major issue. The major parameters were reported to be very weak here the uniqueness was reported to be 1.05% while the reliability was 99.99%. An improved version [33] of the same arbiter PUF model was reported to be with 23% uniqueness and 99.35% reliability.

This PUF model was successfully attacked and broken using side-channel attacks [32]; the Basic Arbiter PUF scheme is 96.45% predictable for over 5000 CRPs. Another proposed model for resisting side-channel attacks [34] was proposed by placing MUX in parallel and by using XOR to generate responses. This technique was subjected to side-channel attacks and was broken with a prediction rate of 99% for 60000 CRPs, which is an absolute increase from the general mode[35] [15].

2.3.2 Ring oscillator PUF

Fig. 2.6 represents a basic ring oscillator PUF as proposed in [2]. A ring oscillator PUF is one another unique design module for PUF design exploring its frequency stages, i.e., the initial stage of the frequency cannot be determined, or it is simply

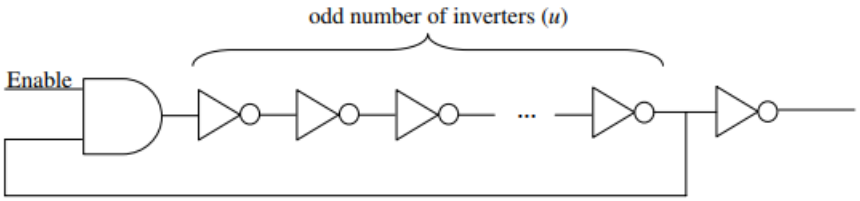

Figure 2.5: A basic ring oscillator circuit

random. Ring oscillators [2] in general are a series of inverters in a feedback line, as shown in Fig. 2.6.

It comprises of N identical inverter connected in a series form and then a feedback loop, to form a ring oscillator structure. Here each inverter has its own delay factor, creating a random stage for the cascaded form. Then each RO module (N-oscillators) is connected to N multiplexers, where each selection line is its challenge bit.

The output of the multiplexers is connected to a counter, which acts as clock inputs of the counters. After the counter starts counting, the counter outputs are compared. If the upper counter has a higher value when compared to the lower the output resides as 1, otherwise 0.

Process variations and mismatch play a vital role in the performance of Ring Oscillator PUFs. A pair of ring oscillators which produce more unlikely different output tends to have better reliability.

The reliability strongly depends on the difference between the oscillation produced. As an advantage of Ring Oscillator PUF, these could be implemented in hard Marco and instantiated as many times as needed in the top-level design. By using this methodology, all PUFs are identical in terms of placement and routing, and therefore the design time is reduced.

A test was conducted [2] to check the uniqueness and reliability of these PUFs. It was seen that the PUF scheme over 15 FPGA chips showed a uniqueness of 46.15%

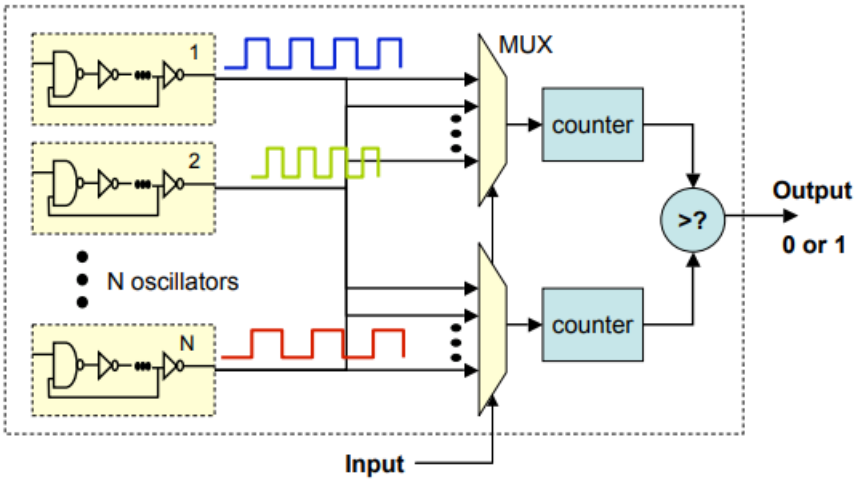

Figure 2.6: Ring oscillator PUF [2]

and reliability of 99.52% under. The main drawback of Ring Oscillator PUF is its high area requirements compared to other models. Ring oscillator PUF was also successfully attacked (extracted frequency [36]) using side-channel attack[37], which creates concerns about its application and strength.

2.4 Glitch PUFs

Most of the combinational circuit logics have a glitch factor. Glitch parameters vary according to the characteristics of the circuit, which in turn directly depend on the fabrication process. Considering the fact that glitch could be used to make unique response bits, this parameter is then used for PUF applications.

Here unwanted parameters are being converted into beneficial factors. Anderson PUF is an example of glitch based PUF [3]. Fig. 2.7 represents Anderson PUF, which is one of the more popular and early models of PUF.

This PUF was implemented using an FPGA $65nm$ on a Spartan-6 [38]. The 64-bit Anderson PUF obtained 45.62% uniqueness. The drawback of this PUF is that it

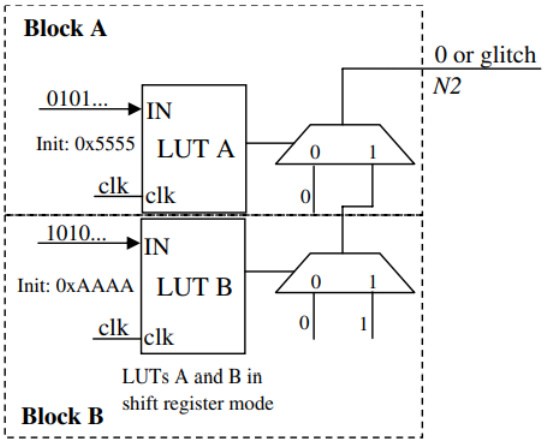

Figure 2.7: Glitch PUF [3]

suffers from instability due to the bit-masking technique [39].

2.4.1 Analog PUF

Analog PUF is a unique model that utilizes device parameters, i.e, usage of mismatch in micro and nano-devices. Ideally when developing a PUF model in FPGA or digital environment, the developer, could only play with its logic factor, not the device internal parameters such as width or length of NMOS and PMOS devices for creating the logics.

A study was conducted [4] developing a model for analog PUF, where the threshold voltage of the MOS device was used as the primary source of variation in the PUF. N-channel transistor, NMOS, was used for developing the delay lines. Fig. 2.8 represents this Analog PUF. The challenges are received at the decoder, which is N to $2N$ configured. The decoder is then connected to the delay boxes were all the boxes are identical to each other, making the NMOS device majority of the transistor types used int he design.

The reason for choosing only NMOS is that the core threat to the design would be HCI (Hot carrier injection) and not BTI (Bias temperature instability). The output

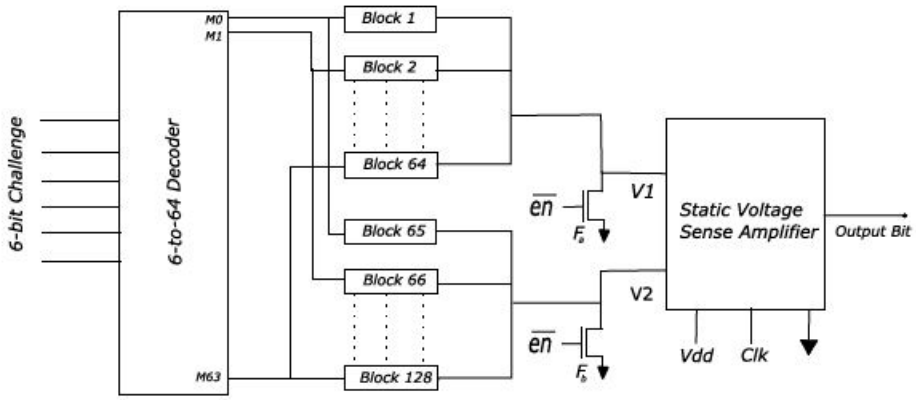

Figure 2.8: An exmaple of Analog PUF [4]

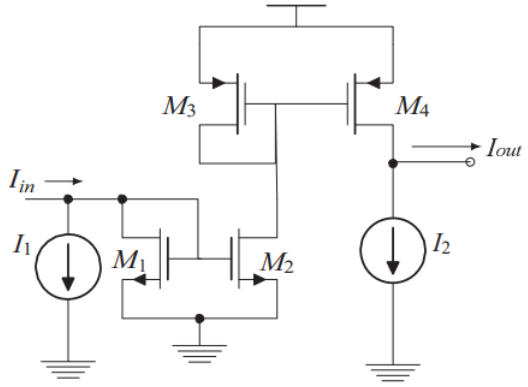

Figure 2.9: Current mirror [5]

is connected to two delay units, as shown in Fig. 2.8. The output of the delay line is then given to a flush transistor and a sense amplifier for boosting the signal as detecting the one which reaches first. The design, for sense amplifier, should be very careful as the amplifier could be sensitive for the output. The design of flush transistors is also very sensitive. The biggest drawback of these transistors is the design of flush transistors; if the previous is not flushed out properly, this could drive the circuit into a High Z condition ie, the output is not being driven to any defined logic level by the output circuit (tri-stated, or floating).

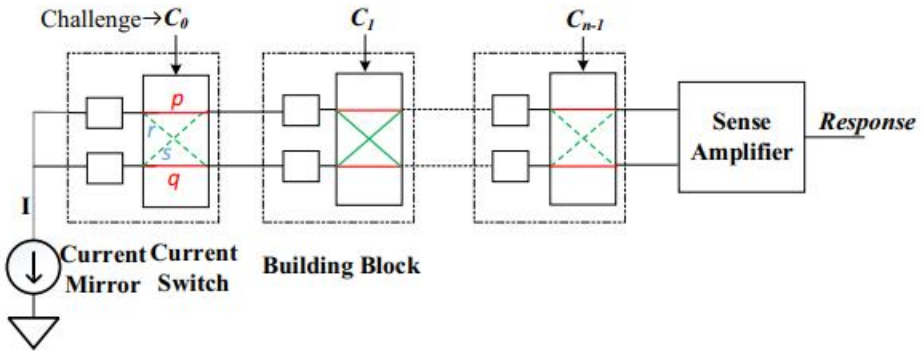

Figure 2.10: Current mirror-based PUF [6]

Another drawback of the circuit is that the design of a sense amplifier is crucial as in real-time environmental factors play a vital role in output as in reliability of the circuit may reduce when compared with others. The Analog PUF [4] is offering 50.02 to 50.10 uniqueness in various nodes, followed by a reliability factor of 96 to 97 in different foundries.

Another model was introduced by [6], which is based on the use of current mirrors and their sensitivity to device mismatch in order to create the randomness. Current mirrors were cascaded in the same form as an arbiter PUF as shown in Fig. 2.10. Current mirrors are designed as in Fig. 2.9. The current mirrors are then connected to a switch boxes p and q, r, and s which acts as zig-zag when challenges are given in. The design is shown in Fig 2.10. Here two current mirror in parallel with their output to the switch box forms a unit. These units are then designed depending on the number of challenges given. If the challenge is 1 channel p and q is formed while if the input challenge is 0 the channel r and s.

The output line is captured using a sense amplifier; this method was found to be very effective as it was cracked by modeling attacks [6]. In [6] it was shown that the CRPs were predicted with ease using a generic algorithm and side-channel attacks. It should be noted that this weakness could be due to the simplicity of the model which similar to delay-based models relies only on mismatch and delay units for its

randomness.

2.5 Mixed-Signal PUF

A group of researchers proposed a PUF model based on current mirrors mismatch [4]. A gate-level representation of this model is shown in Fig. MixedPUF. The model uses complementary current mirror circuits were the output is pulled from Y, as shown. Y produces a random output due to mismatch in the circuit; the output is then given to a buffer circuit for amplification [4].

This work fused the two PUFs for better strength in creating randomness. The circuit has been implemented in $65nm$ technology. Although the PUF is performing better, it suffered from a major drawback. In this design, the buffer stage at the output cannot suppress bit inputs, and hence circuit noise level goes high [7]. To improve this the same research group implemented an upgraded version of the design, which was based on using a series of current mirrors that were used with a cascaded complementary current mirror for increasing stability. Meanwhile, the outputs were given to a hysteresis circuit for further process.

Using the $40nm$ technology node, a test chip was designed and tested over 25 degrees to -85 degree and ran $100,000$ Monte Carlo simulation and was able to achieve 49.07% uniqueness and 99.9951% reliability during its test. Most interestingly the energy consumption was estimated to be 1.02 FJ/bit.

A similar model was proposed by [40] which has an overall power consumption of 124 FJ/bit with a uniqueness if 49.94%. This model [40] was reported to have better a reliability figure-of-merit (RFoM) 1.53 and 2.56 respectively when compared to [7].

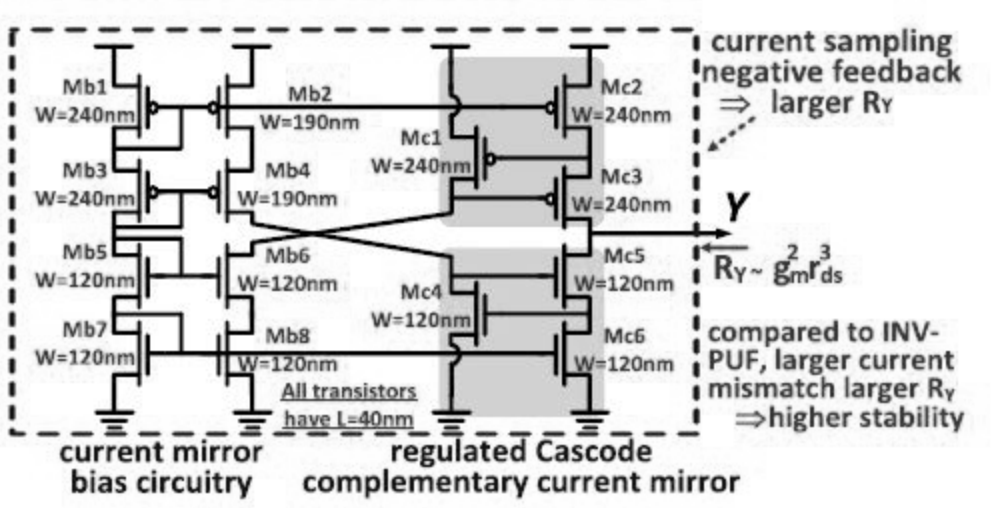

Figure 2.11: Current mirror cascaded with regulated Cascode complementary current mirror (RCCM) [7]

2.6 Memory based PUF

Memory-based PUF exploits the usage of metastability in circuits. A simple configuration of an SR latch is shown below in Fig. 2.12, which shows the gate-level design of a PUF based on the SR-latch.

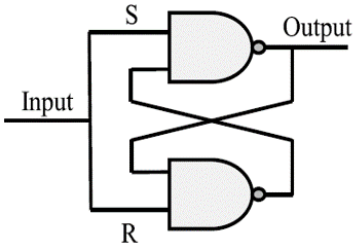

Figure 2.12: Conventional SR latch [8]

SR-latch is designed using two crosses coupled NAND gates as shown in 2.12. When both the inputs are fed with high signals (rising edge), the latch enters a metastable state and starts oscillating. Ideally, if the feedback loop is designed iden-

tically using two NAND gates and symmetric routing the SR-latch keeps oscillates continuously in a metastable state.

Due to natural random variations, one of the feedback loops is stronger than the other and hence the SR-latch stops oscillating and settles on to a state. The state that SR-latch gets settles is totally unknown and it completely depends on the delay and the feedback loops [41]. This could be used for generating responses for PUF applications.

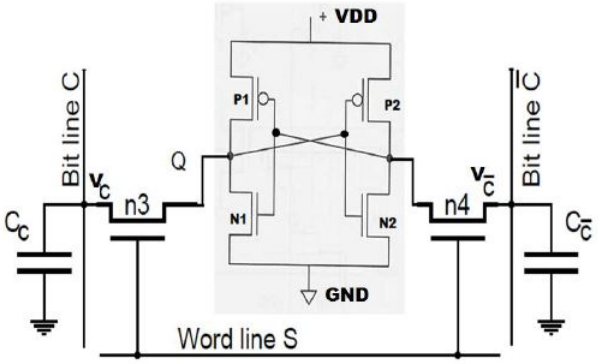

Figure 2.13: Conventional SRAM [9]

SRAM cells are also used to built PUF models [42]. A typical SRAM has two inverters connected, as shown in Fig. 2.14. All inverters are designed in such a way that it should be properly matched. However, due to fabrication variation, this is not possible, and at least one inverter could be stronger ie, due to random mismatch one inverter could behave faster than the other. During the power-up phase, the memory cells get settled by the stronger inverter. If the difference between these is not significant, the output could be an unstable bit (metastable); if it's significant, then the results could be stable.

The drawback of the memory-based PUF is that cells should be repowered whenever the response is needed [43]. The power-up state of 8190 bytes of SRAM from different memory blocks on different FPGA boards was collected in [25]. The uniqueness is reported to be 49.97% and the reliability is shown to be 96.43% at normal

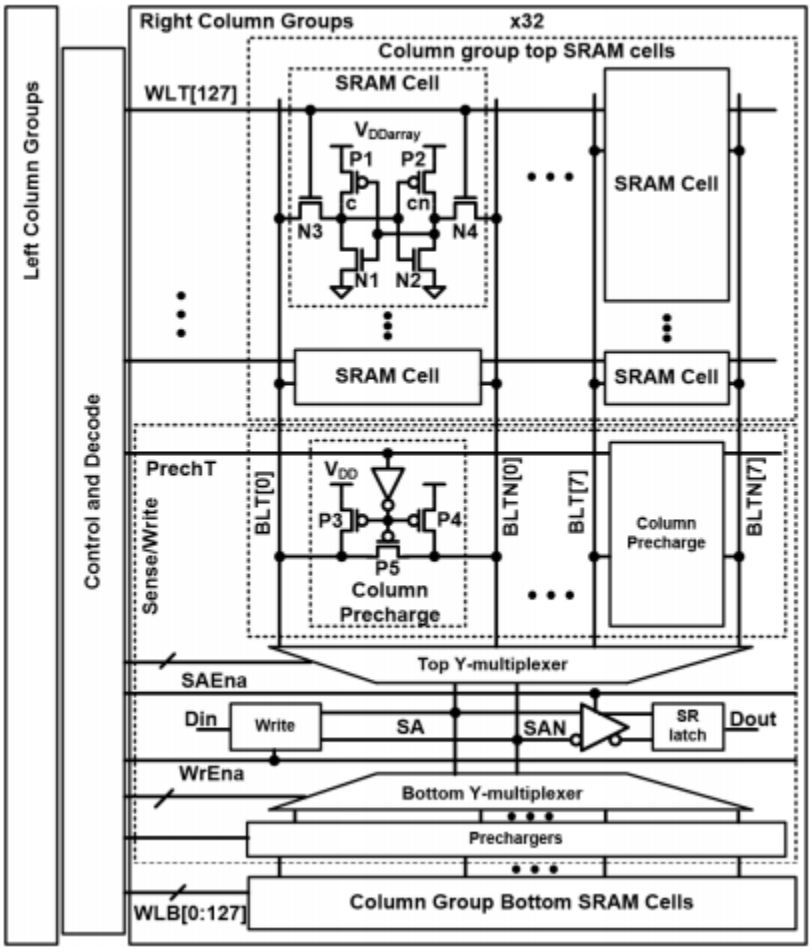

Figure 2.14: The basic configuration of SRAM PUFs. [10]

conditions and 88% for higher temperature conditions. Few other similar PUF models are butterfly PUF, Bus keeper PUF, etc. Implementation of butterfly PUF was conducted in the FPGA platform, and uniqueness was obtained of about 50% and reliability of 95%. In contrast, bus keeper implementation was estimated to be 48.88%, the reliability is reported to be 95.84% [44].

Fig 2.14 represents a general model for SRAM PUF. Here a control and decode unit is used to receive the challenge pairs. The output of the decoder is given a write line of the PUF (WLT). The model is designed in a way such that it has a 32 column and 128 rows. The SRAM is triggered using a pre-charge circuit for its read and write lines (BLT, BLTN). The output of the pre-charge is then given to a multiplexer. Similarly, a second-half unit is designed at the bottom which carries another 128-bit row and 32-bit column. Both multiplexer outputs are then connected to an SR-latch response output.

2.7 Comparison of Different PUF Models

Table 2.2 summarizes the conclusion made in the literature survey.

Table 2.3 summarizes the survey conducted in chapter 2. Here the table evaluates the uniqueness, reliability, and power consumption of PUF units.

One main issue with most of the developed PUF is that these works do not consider the power consumption required for the PUF. In fact, many of these PUFs are not suitable for sensor technology or RFIDs. Therefore, the objective of many of these works which have been RFID is not fulfilled. As noted, the analog TV PUF has the lowest noted energy consumption in the research conducted with a comparable uniqueness and reliability close to the ideal value.

Sl no.	PUF type	Draw backs
1.	Arbiter PUF	1. Uncontrolled routing procedure and is not feasible to implement a fully symmetric arbiter on FPGA. 2. Traditional arbiter PUF is vulnerable to machine learning based modeling attacks due to its linearity.
2.	Analog PUF [4]	1. Current mirror-based arbiter PUF. 2. PUF is not strong enough to resist modeling attacks.
3.	Static Monostable [7]	1. The limitation for the model is that few cases for the mismatch between these current mirrors is very close to zero. This significantly reduces the quality of the output. 2. The skewed inverter model cannot suppress these bit flips at the current mirror is highly sensitive to noise.
4.	Ring oscillator [36, 37]	1. Lock on the same frequencies by changing the supply. 2. Frequencies of ROs were extracted and their locations inside the chip using the electromagnetic side channel analysis.

Table 2.2: Drawbacks of different PUF types

Serial No.	PUF scheme	Uniqueness	Reliability	Energy consumption (FJ/bit)
1.	Arbiter PUF [33]	1.09%	99.99%	NA
2.	Arbiter PUF [15]	23%	99.35%	NA
3.	Ring oscillator [2]	46.15%	99.52%	NA
4.	Analog TV-PUF [4]	50.02% to 50.10%	96% to 97%	1.81
5.	Static Monostable [7]	49.07%	99.9951%	1.02
6.	Static Monostable [45]	50.10%	99.9943%	15

Table 2.3: Comparison of different PUF models with its parameters

2.8 Conclusion

This section describes the overall literature of different PUF topologies and their drawbacks. This section also intents to focus on the need for low power PUF devices for applications such as IoT. Energy consumption per bit has been summarized in table 2.3. This thesis proposes a novel design focusing on less energy consumption.

Chapter 3

Implementation of PUF models

In this chapter, the design and implementation of the proposed PUF will be presented. The implementation of the PUF is evaluated based on several performance merits, such as Reliability, and Uniqueness. Moreover, its power consumption will be compared with the state-of-the-art architectures.

3.1 Figure of Merit of PUF

In this section, we briefly discuss more the important properties of PUF. These parameters which include uniqueness and reliability is being considered for measuring the performance of the PUF.

3.1.1 Reliability

This parameter is primarily used to find the ability of the device to reproduce the same response under different conditions. Ideally, the value should be 100%; due to natural effects such as temperature, electromigration, etc., the device may not be able to reproduce the same values as such [46].

This evaluation parameter is obtained as follows:

$$Reliability = (1 - \frac{2}{m \times (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{HD(r_i, r_j)}{a}) \times 100\% \tag{3.1.1}$$

where m represents the number of response samples, a is the number of response bits, and Hamming distance (HD) is the distance between two response samples, in

equation r_i and r_j.

3.1.2 Uniqueness

Uniqueness is one of the most important parameters for the PUF unit. The uniqueness of a device can be measured by giving the same challenge to two different PUF devices and capturing the output. Ideally, the two outputs should be different ie, Ideally, this value should be 50%. [46].

The uniqueness of a PUF is evaluated as follows:

$$Uniqueness = \frac{2}{g \times (g-1)} \sum_{i=1}^{g-1} \sum_{j=i+1}^{g} \frac{HD(r_i, r_j)}{a} \times 100\% \tag{3.1.2}$$

where m represents the number of response bits, g represents the number of PUF instances under study. Hamming distance (HD) is the distance between two response samples, in equation r_i and r_j.

These two parameters, along with the power consumption of the PUF will be used for comparison purposes. The power consumption dictates the application of the proposed PUF in low power sensor network application and is one of the most important design criteria.

We will show that the proposed PUF, with a novel design of the SR-latches, results in very low power consumption, making it a suitable candidate for this end application.

3.2 Proposed design

The proposed model is composed of both digital and analog circuits, which can create a higher level of randomness. The proposed design is shown in fig 3.1. It has n number

of multiplexers that accepts the challenge signals, in which the output of each MUX is connected in a zig-zag manner, to generate the output.

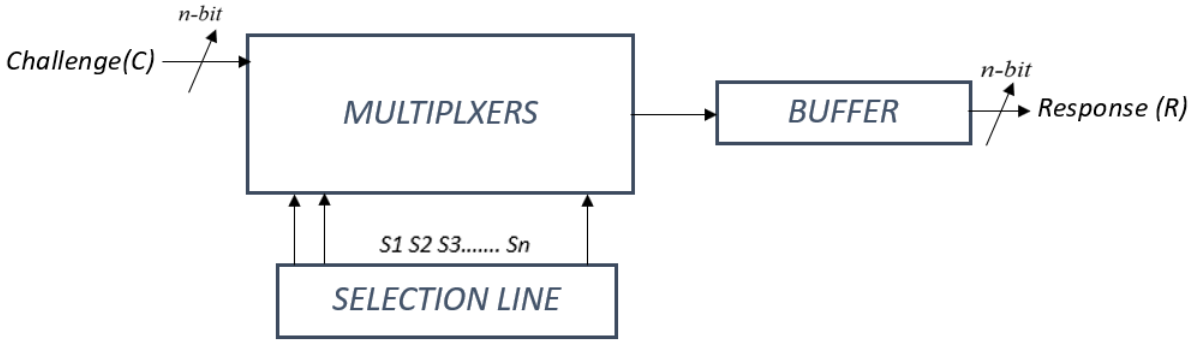

Figure 3.1: Proposed design

The selection lines are controlled by a novel SR-latch unit, which is configured in its metastable states for random output, followed by a coincident flip flops for higher bit stability and randomness. The multiplexers are triggered using these unique values, and the output of MUX is given to a buffer stage to create the desired output and set the output voltage to level, proper for the digital format.

The proposed design is fully custom-designed using the Cadence environment and in the TSMA 180 nm technology node. A full and detailed version of the PUF model will be presented in the next Chapter.

As will be described, the design would be an initial model for partial automation of larger PUF.

3.2.1 PUF Results

Here Cadence virtuoso IC 5.1.4 was used for all simulations and design methodologies, including schematics and layouts. The transistor models are based on the TSMC models. This section gives an outline of the whole software-level implementation flowchart and final tests.

Design Procedure Flow chart

Fig. 3.2 represents a simple flow chart of the design procedure used in this thesis. As the first specifications were set, a literature survey was conducted and finally laid a floor plan for the entire design.

The initial tests were carried out in the Cadence Virtuoso schematic design tool, saved, and the Analog Design Environment was used to set it up. The Spectre spice models which were based on the TSMC data were was used for transient analysis; if there is no error, we proceed to the next phase of the design, i.e., layout.

In the second phase, once the requirement is met, layout design proceeds. Once the layout is accomplished, we go for physical verification, which includes DRC and LVS checks.

The DRC check is a Design Rule Check while LVS is Layout Versus Schematic check. The DRC has a set of rule files that are custom built and made by the TSMC foundry. Once the layout is designed, the software compares it with the rule files and matches it with the one made.

Once the DRC check is cleared with no errors, then we continue with the same extraction and then conduct LVS. If any errors are found in DRC or LVS, we send it back to the layout to fix it. Finally, after extraction, a schematic is formed which includes all of the parasitic elements in the circuit and is used for final and post-layout simulations.

3.3 Proposed PUF Performance analysis

The test for the proposed PUF was conducted using Monte Carlo analysis and then fusing multiple PUF models for creating a 4-bit model. Fig 3.3 is shown below, which represents the plot for tests.

In this work, first, a 4-bit PUF basic model was used. This basic cell was later used to expand the input/output bit numbers to 8, 16, 32, and 64 bits.

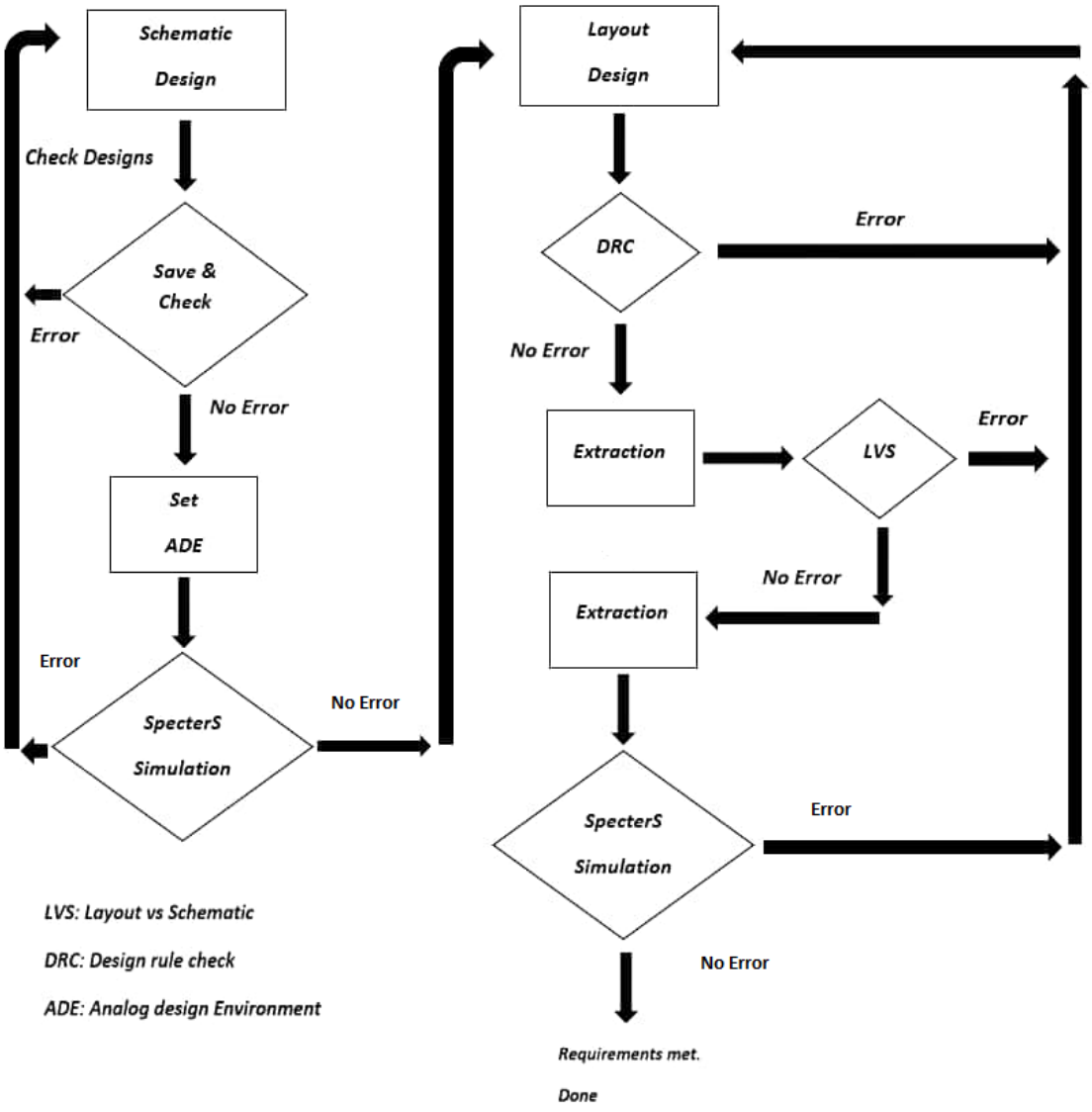

Figure 3.2: Flowchart

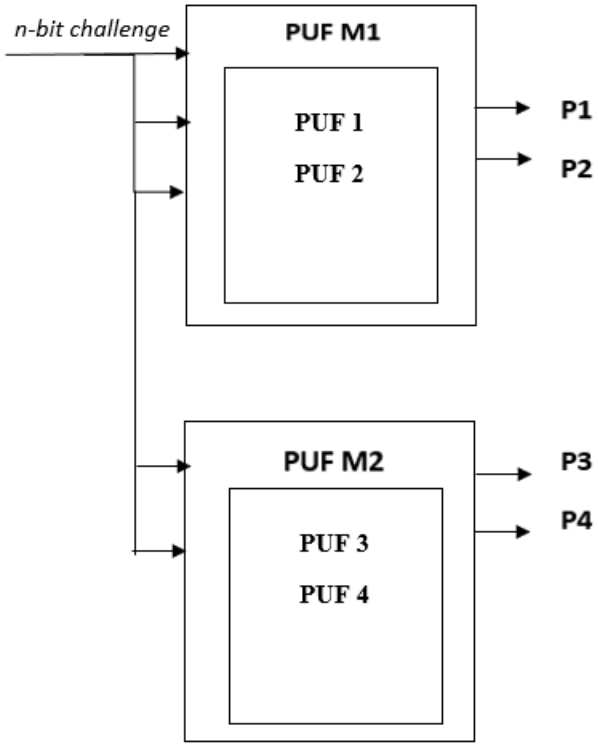

Figure 3.3: Proposed PUF for test

Here in Fig. 3.3, the first block represents PUF $M1$, which consists of four different PUF units with changes in width (PUF) found using parametric analysis. Each PUF in $M1$ block behaves uniquely depending upon their changes in their width. The change in width proportionately affects the performance of the device. This evaluation was found using parametric simulations. PUF $M2$ represents another four-set of PUF units fused with the same challenges, and these are then considered as a single 4-bit PUF model.

The hamming distance is calculated using the values obtained at the output of PUF $M1$ and $M2$, then both are compared, and uniqueness is calculated. Using this technique, n-bit could be easily be developed.

For calculating the Hamming Distance, analog values obtained at each output were rounded up to the nearest digital value. This activity was carried out using

Microsoft excel.

3.3.1 Uniqueness and Reliability of the Proposed PUF

The uniqueness of the proposed PUF has been calculated using three PUF units, which is fused into one PUF model. Similarly, 2 PUFs are used to study uniqueness for the devices. We now compare the two devices for 2-a bit each. The Monte Carlo analysis is done for each PUF unit and the comparison. Approximately 1200 samples were extracted from the Monte Carlo simulation to study reliability and uniqueness. Intra and Inter hamming distances were also calculated using the same CRPs obtained from the extraction.

Proposed 8-bit PUF

The uniqueness is calculated for an 8-bit PUF by using the final extraction file, and then using the ADE tool, the outcome of the Monte Carlo analysis was studied and plotted.

Fig. 3.4 represents the Monte Carlo (MC) analysis for process variations and $1,000$ iterations. The Hamming Distance (HD) is plotted in Fig. 3.5, where the x-axis represents challenges given while the y-axis represents the value of the Hamming Distance. The uniqueness of the 8-bit PUF is calculated to equal to 50.55%, and reliability is 99.504%.

However, a 4-bit PUF is not useful, and it was created for the construction of the higher digits PUFs. We have evaluated the merits of the PUF at each stage to make sure that the final PUF is secure.

Proposed 16-bit

The same approach was used for evaluating the performance of the 16-bit PUF. Fig. 3.6 represents the MC analysis for process variations for $1,000$ iterations, and the

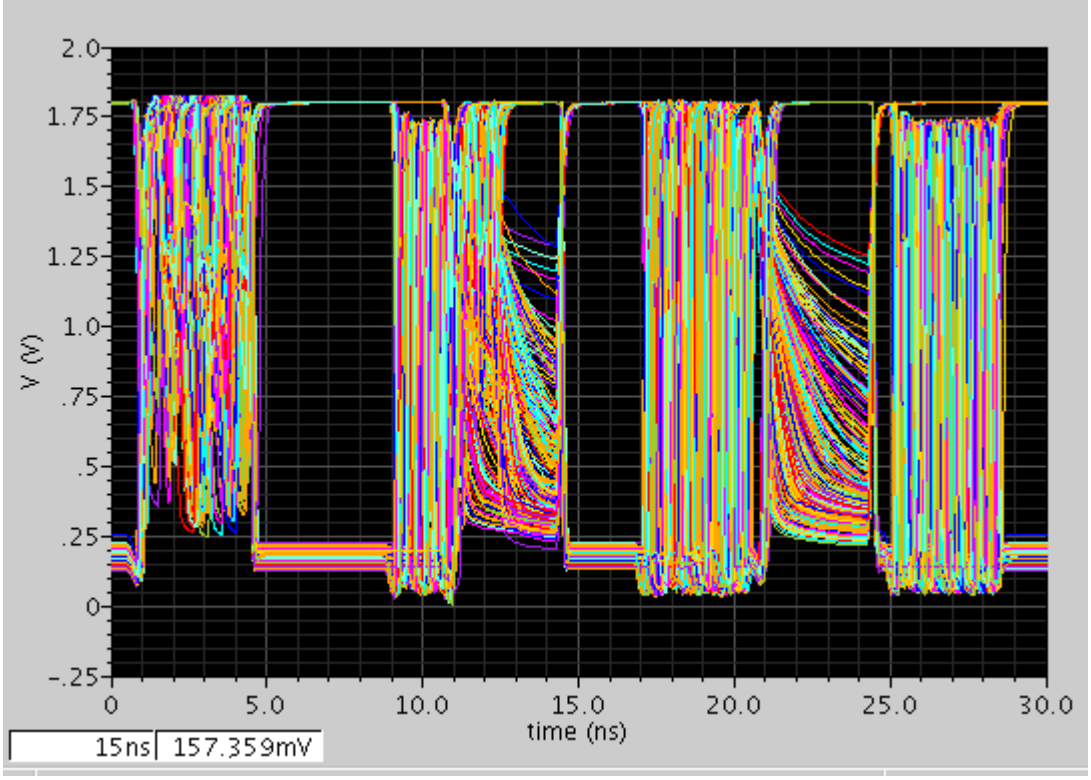

Figure 3.4: Monte Carlo analysis for 8-bit PUF

calculated Hamming Distance is plotted in Fig. 3.7, where the x-axis represents the given challenges, while the y-axis represents the Hamming Distance. The reliability is 99.337%, and the uniqueness is equal to 49.68% for the 16-bit PUF.

Proposed 32-bit PUF

The uniqueness is calculated for 32-bit PUF using the final extraction file and then using the ADE tool for performing the Monte Carlo analysis. Fig. 3.8 represents the $1,000$ iterations of the MC analysis with process variations.

The uniqueness of 32-bit PUF is estimated to be 48.96%, and its reliability is 99.012%.

The calculated Hamming Distance is plotted in Fig. 3.9, with the x-axis representing the given challenges, while the y-axis representing the Hamming Distance.

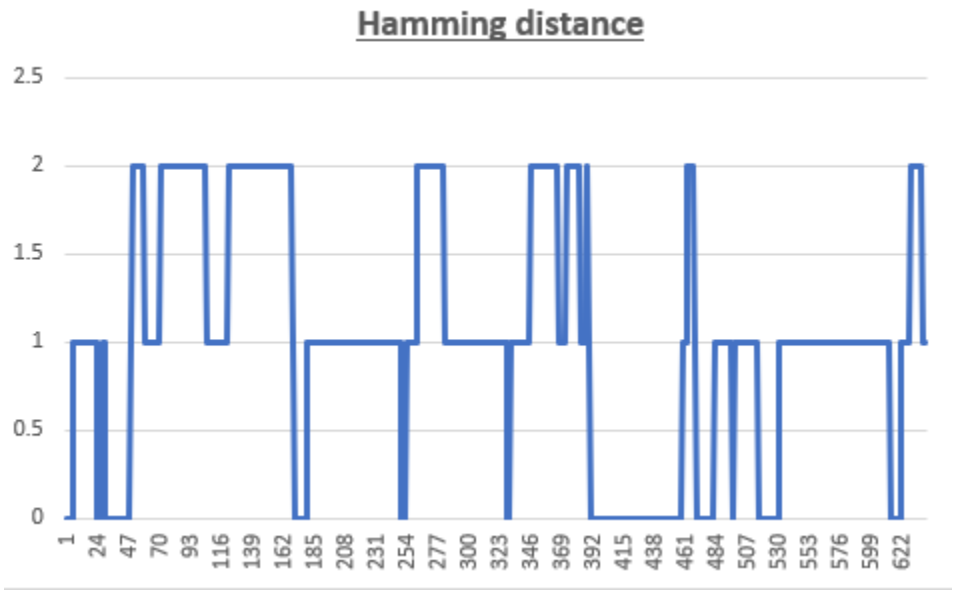

Figure 3.5: Hamming distance for 8-bit PUF

The Proposed 64-bit PUF

the 64-bit PUF was generated using the lower digit cells and was tested for its uniqueness and reliability. Fig. 3.10 represents the MC analysis for process variations for $1,000$ iterations.

The Hamming Distance is plotted in Fig. 3.11, where the same as before, the x-axis represents the given challenges, while the y-axis represents the Hamming Distance.

The reliability of the 64-bit PUF is estimated to be 99.788%, and its uniqueness is equal to 48.68%.

The result of the developed PUF are summarized in Table 3.1.

3.4 Power and Delay of the PUF

To measure Power, the circuits were marginally adjusted by inclusion of a passive device (0 (V) DC), which won't influence the circuit and associate it to power supply node (*vdd*) of the block through the negative terminal and interface the positive node

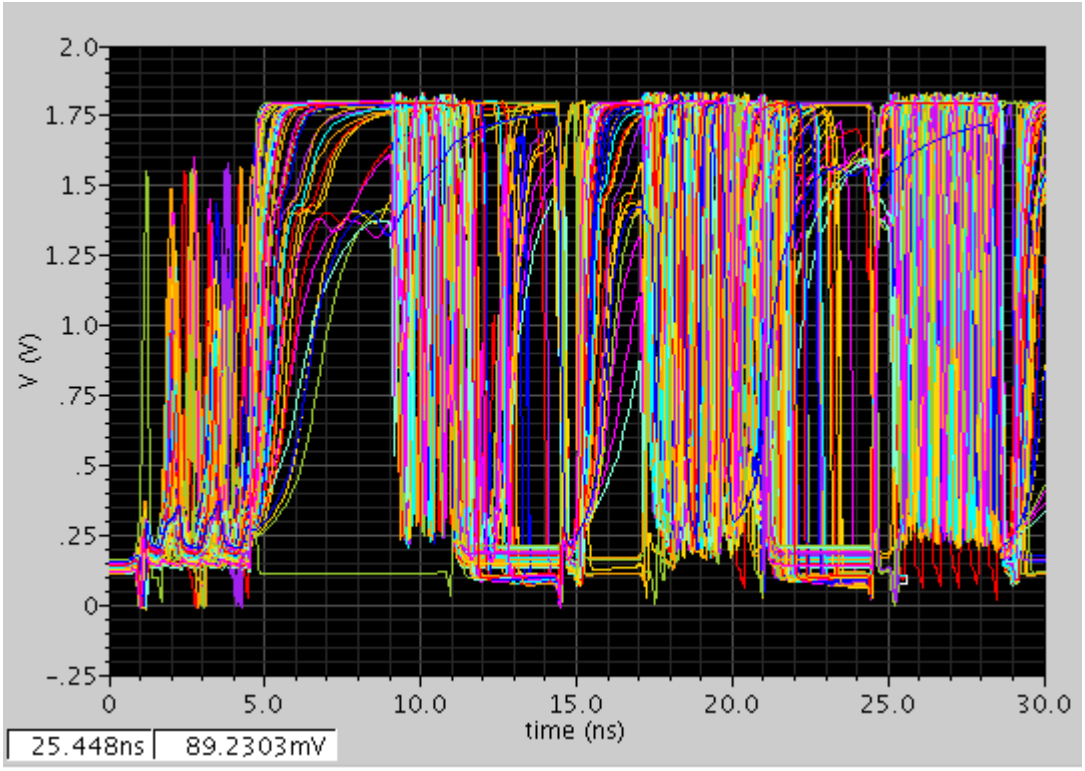

Figure 3.6: Monte Carlo analysis for the 16-bit PUF

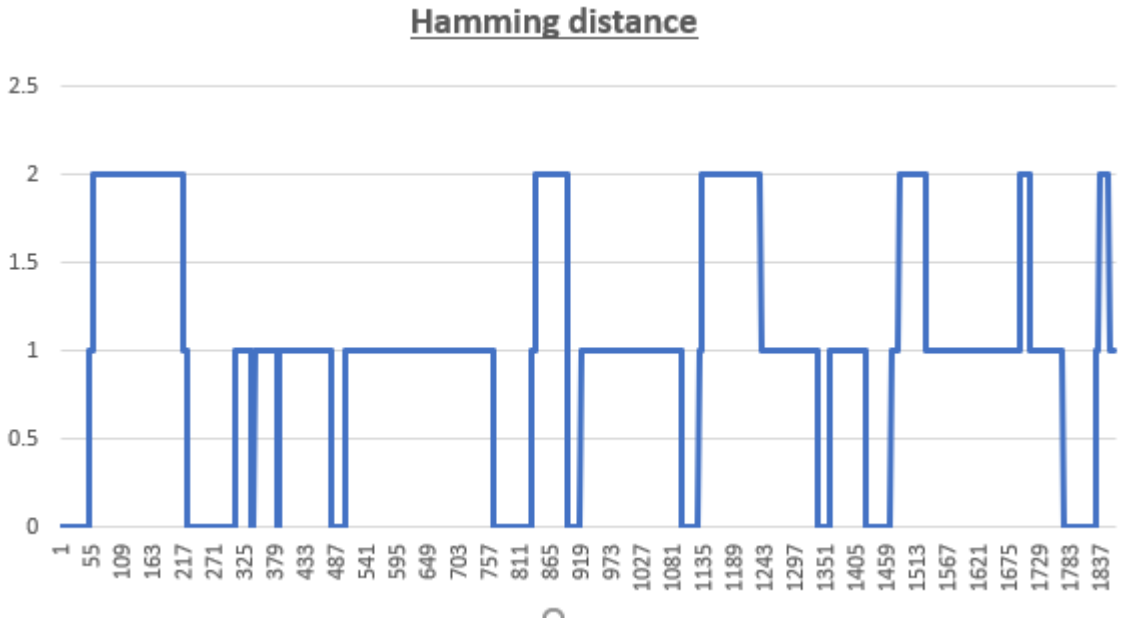

Figure 3.7: Hamming distance for 16-bit PUF

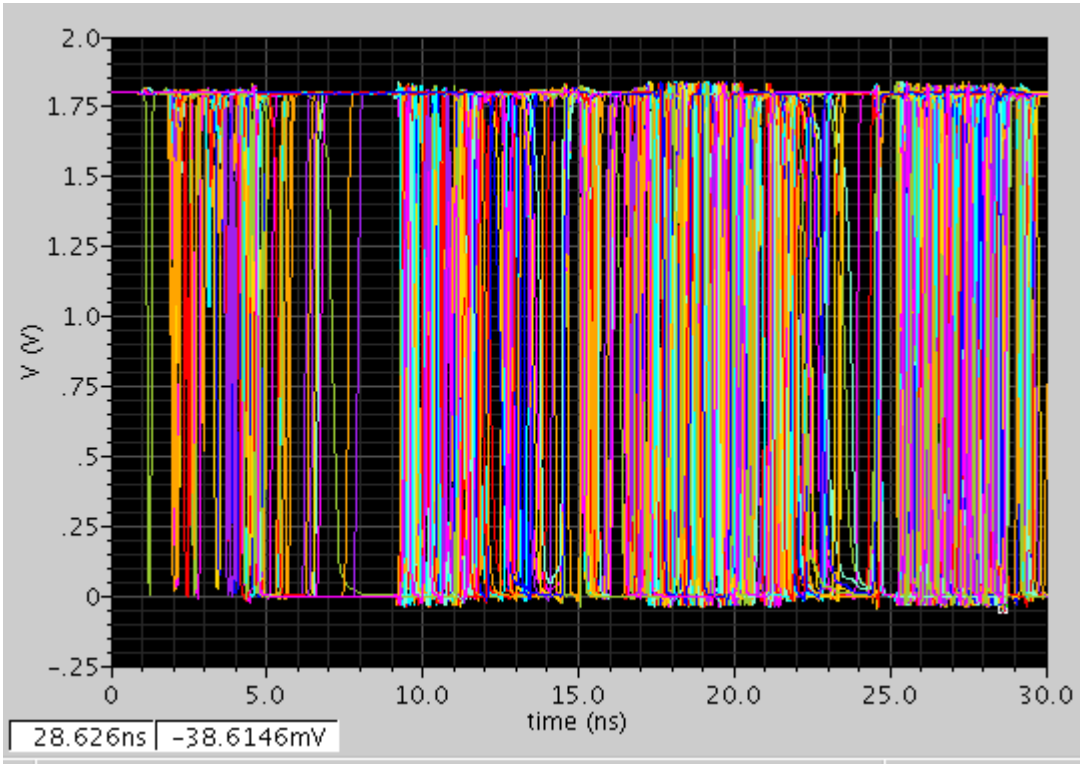

Figure 3.8: Monte Carlo analysis for 32-bit PUF

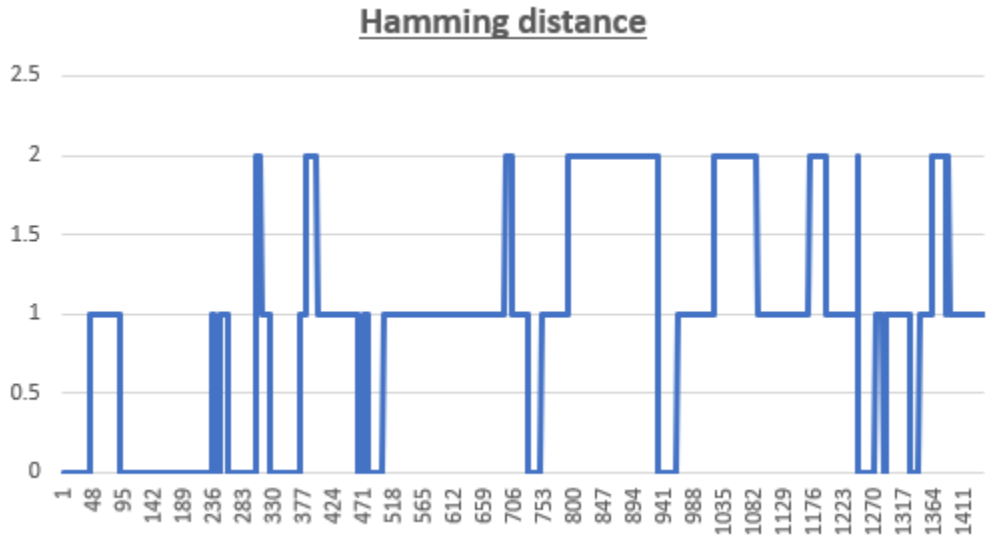

Figure 3.9: Hamming distance for 32-bit PUF

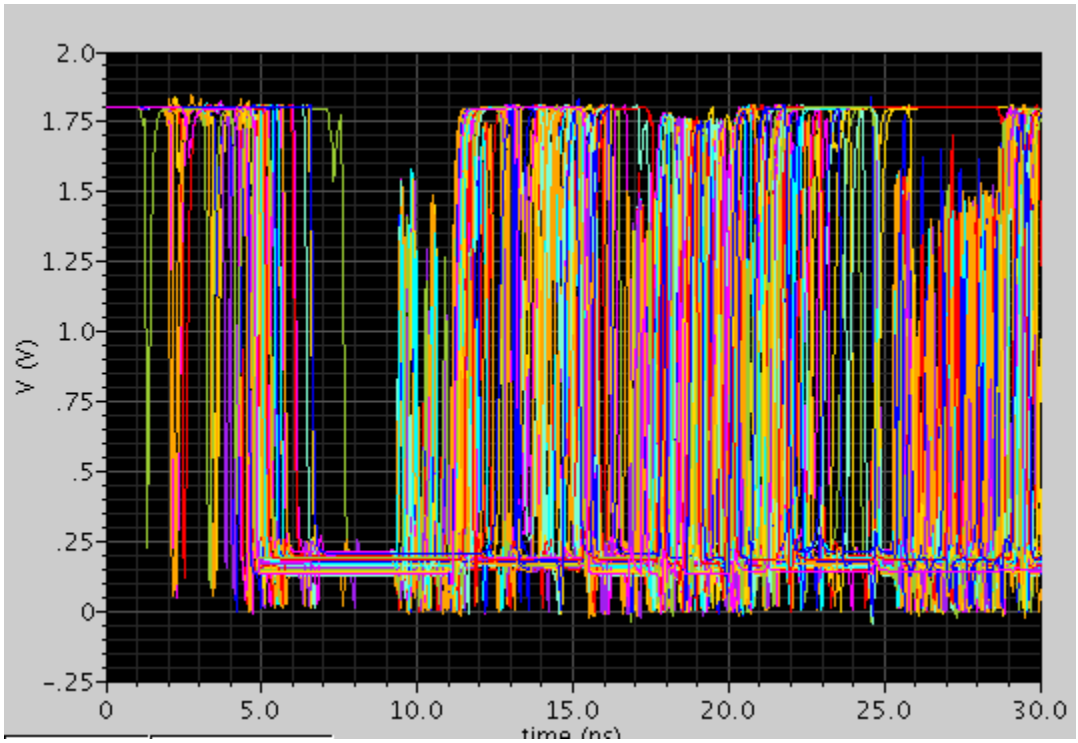

Figure 3.10: Monte Carlo analysis for 64-bit PUF

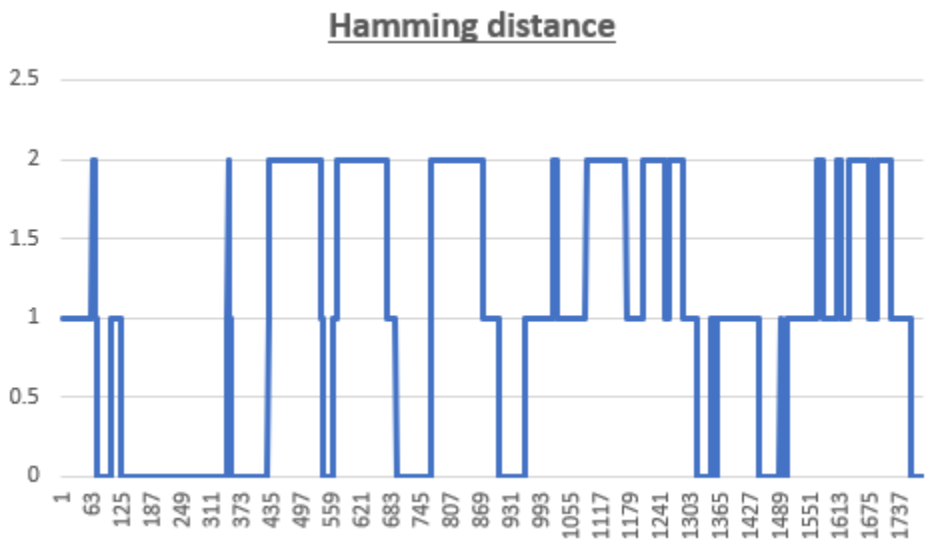

Figure 3.11: Hamming distance for 64-bit PUF

to ground (*gnd*). By using the "integ" command, the Power was measured. For the delay calculation, we used the calculator directly for finding the desired parameter.

3.5 Comparison study

Table 4.2 represents a comparison study made with few published models.

The proposed design aimed to present a low power PUF unit that could be widely used in IoT devices. The design is incorporated with standard cell-based design flow; this methodology could be used to develop larger PUF units with basic standard cell blocks (P-cell) when compared with conventional design techniques. The standard cell approach provides the designer the ability to submerge the PUF core on to the basic cells, which allows natural obfuscation.

Here we have introduced a better design when compared to [7] and [45]. The limitation of this model is that few cases for the mismatch between these current mirrors are very close to zero. This significantly reduces the quality of the output. The skewed inverter model cannot suppress these bit flips at the current mirror is highly

No.	Uniqueness	Reliability
8-bit	50.55%	99.504%
16-bit	49.68%	99.337%
32-bit	48.96%	99.012%
64-bit	48.68%	99.788%

Table 3.1: Reliability and uniqueness values of the final 64-bit PUF and its associated sub-cells of 32, 16, and 8-bit PUFs

PUF type	[45]	[4]	[7]	**Proposed**
Year	2016	2016	2018	2020
Process (nm)	65	90	40	180
Topology	Static monostable	Analog TV	Static monostable	Analog-mixed
Uniqueness	**50.01%**	50.10%	49.07%	48.68%
Reliability	99.9943%	97%	99.9951%	**99.748%**
Power (microwatts)	NA	0.180@1GHz	NA	**0.01124@1GHz**
Energy consumption per bit (Fj/b)	15	1.81	1.02	**0.1130**
Delay	NA	NA	NA	3.586E-9
Standard cell design	NO	NO	**YES**	**YES**
Area per bit @40nm (normalized)	8.18	NA	**5.83**	8.037
Number of challenges (CRPs)	NA	64	NA	64

Table 3.2: Comparison study

sensitive to noise. The proposed design has bypassed these effects. The proposed design has a PUF core similar to [7] and [45]. Both the PUF core has a single unit of random generation units within them i.e. if a slight change to the main block could affect the whole parameters of the PUF. Here instead of one core, we have introduced multiple cores so as if one fails (IR, Antenna, EM, or any environmental issues, etc.) the other core picks it up and processes it.

[4] has a very highly sensitive sense amplifier and flush transistors ie, the whole performance of the device depends on these models. The design of sense amplifiers is

one of the most crucial steps and it could be affected by various environmental factors. The proposed model was designed considering all these factors and was introduced a standard cell automation technique for the development and its design. This could ease the designer from developing from the scratch of any design.

The proposed model is the lowest in terms of energy consumption which in turn is ideal for IoT devices or low power applications. Other PUF parameters such as uniqueness and reliability are also comparable with the other published results.

Chapter 4

Design Details and Sub-Circuits

In this chapter, cell designs of the proposed PUF are presented. The circuit-level designs are all tested at the schematic level, and when the functionality was met, full custom layouts were laid out. A new SR-Latch is introduced which operates with low power area requirements.

4.1 Multiplexer design

The proposed MUX, with its selection line generators, are shown in Fig. 4.1. In Fig. 4.1, A and B are the two input lines, while S and $Sbar$ act as the selection line. When S goes high, $NMOS1$ turns on, and $NMOS2$ is off. The MUX is designed using pass transistor logic and is based on the NMOS transistors.

In MOSFET transistors, structurally, the most found issues are hot carrier injection (HCI) and bias temperature instability (BTI). The PMOS transistor is more vulnerable to the negative effects of temperature instability, while NMOS is more affected by the positive bias temperature [4].

The NMOS is chosen here in the design because the constraints affecting the design would only be the HCI effect.Both HCL and NBTI influence the device for the rise of threshold voltage (Vth) over time. PBTI comes into picture only when high gate oxides are used. Here, in this design, a majority of NMOS transistors are used as a result the core threat of reliability would lt be HCI (hot carrier injection) effect.

The used MUX is a threshold voltage modified triggered circuit, which suffers from variations during manufacturing. However, in this context and for the proposed design

S	Sbar	a	b	Out
0	1	0	0	0
1	0	0	1	0
0	1	1	0	0
1	0	1	1	1

Table 4.1: Multiplexer truth table

this fault is advantageous since it creates variations during the process variation. The MUX is in the cascade and parallel mode.

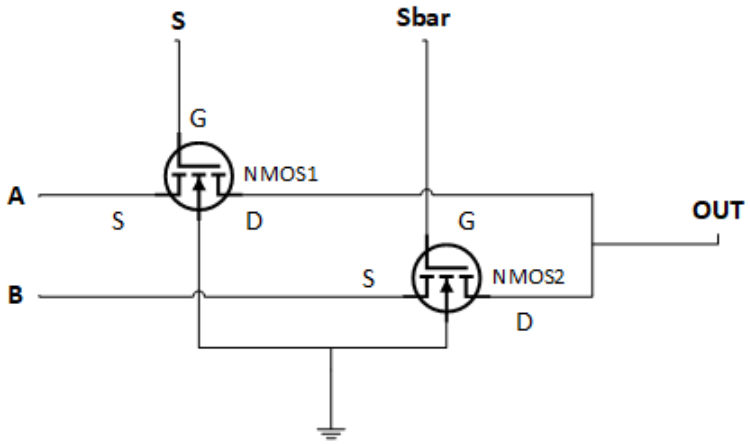

Figure 4.1: MUX using pass transistor

The biggest challenge here in the design of the MUX is to have a design that results in a PUF with high reliability and uniqueness. This will be achieved by introducing a random selection line generator for triggering the MUX units. The functionality of the MUX is shown in Table 4.1

4.2 Selection line design

The entire selection lines are made as a single P-cell design with a combination of SR latch, delay lines, and coincident circuits. SR latch is a novel structure made followed

by NMOS delay lines and 4-bit coincident circuit.

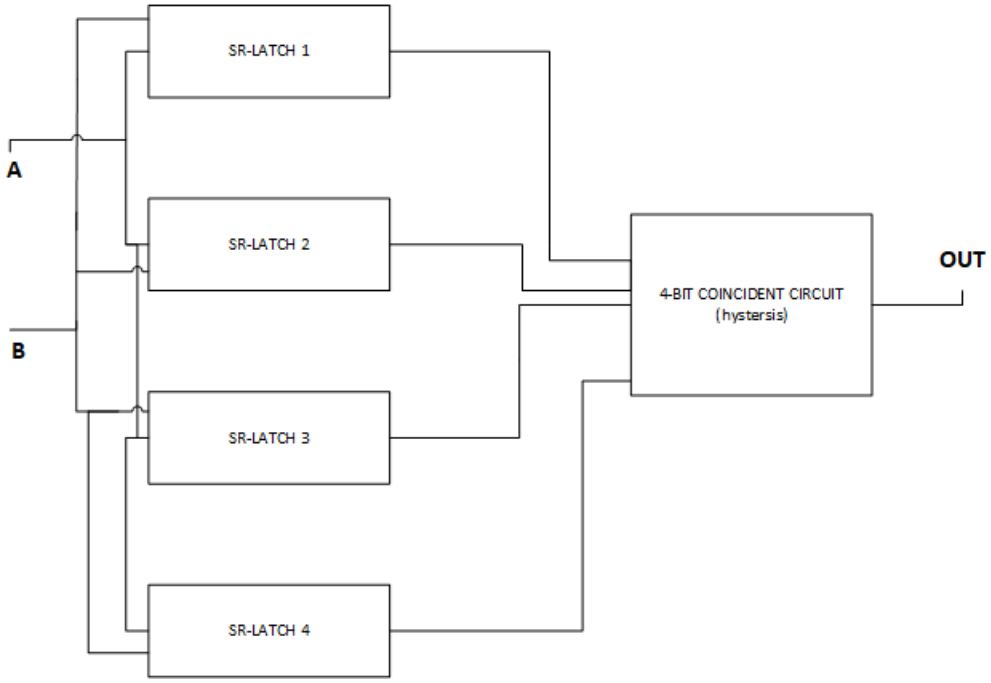

Figure 4.2: Selection line outline model

4.3 SR Latch

In the proposed design of the PUF, the power consumption requirement was one of the major design contrasts. Optimization of the combinational logic circuits is one method used here to save area and power. hence making the proposed PUF suitable for sensor networks.

The SR-latch is made form the AND and NAND gates, as shown in Fig. **??**.

4.3.1 Proposed AND Gate Design

Here we have introduced a novel structure for the creation of logic gates. This proposed and new model uses n transistors for n number of inputs. The result is a circuit

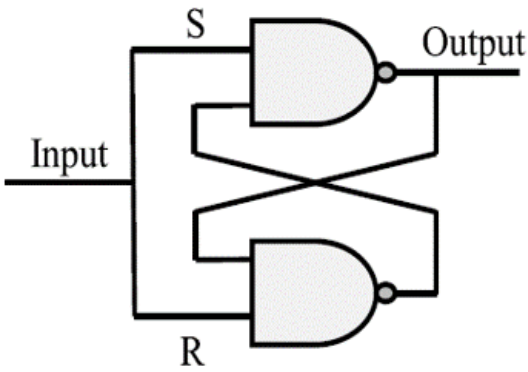

Figure 4.3: SR latch configuration

with reduced area and power requirements. It requires approximately two times less area from the conventional design and consumes approximately four times less power. As an additional advantage, this gate could be used in other applications for efficient performance and its low power requirements.

As an input, the latch is triggered using a clock input, which is shorted to all the data for the locks in parallel. This is made to bring the SR latch into its metastable state. Fig. 4.4 represents the novel AND gate design. Here a and b are inputs, while OUT is the output.

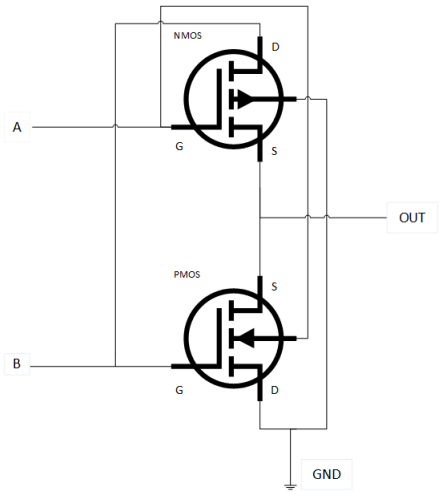

Figure 4.4: Proposed AND gate

The AND gate is designed and simulated in Cadence using the Spectre spice models, and its transient response is shown in Fig. 4.5.

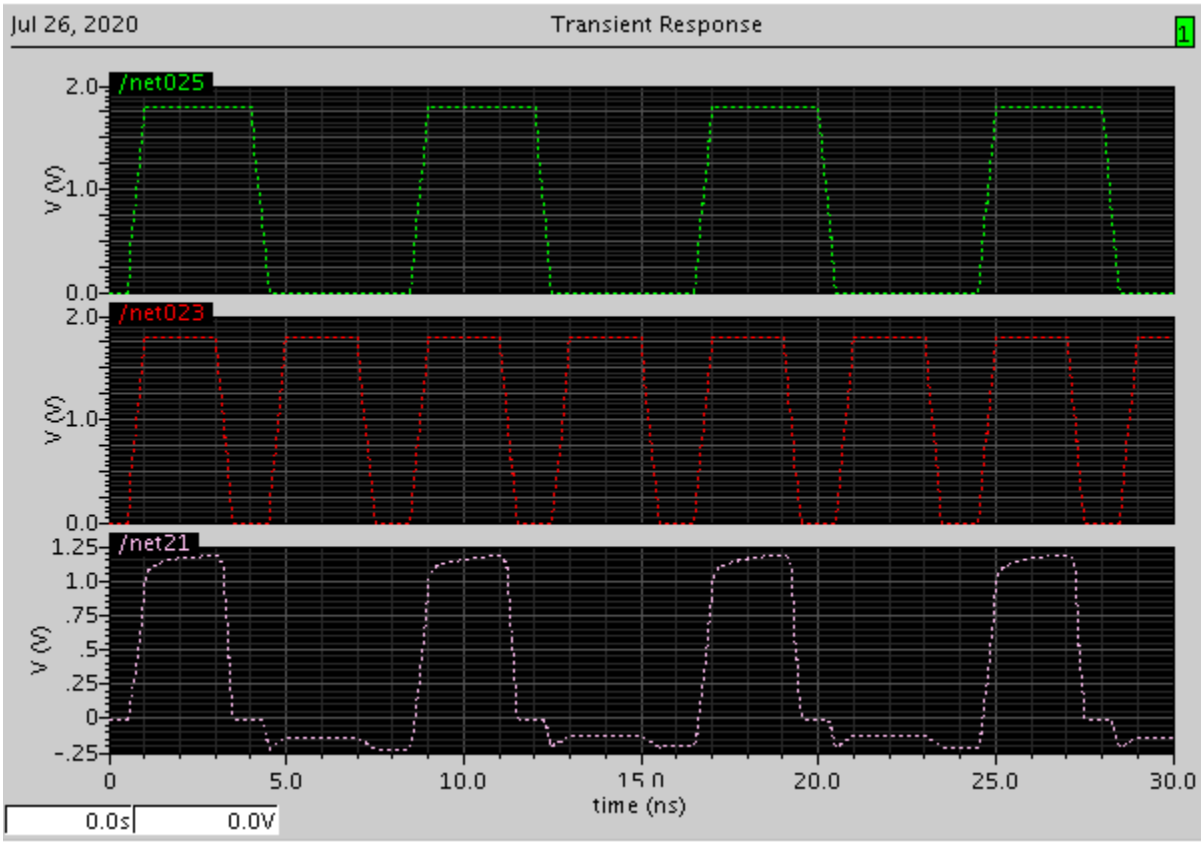

Figure 4.5: Proposed AND gate transient analysis

4.3.2 Proposed NAND Gate Design

The design of SR-latch is being carried out using a NAND gate. A NOT gate is cascaded with AND gate to form the NAND gate.

Fig. 4.6 represents the transistor level of the proposed design. When the output of the AND gate becomes high *NMOS2* transistor turns ON and generates a logic 0 voltage level. When the input is low, *PMOS2* turns ON and *VDD* is passed on to the output terminal, resulting in a logic 1 voltage level.

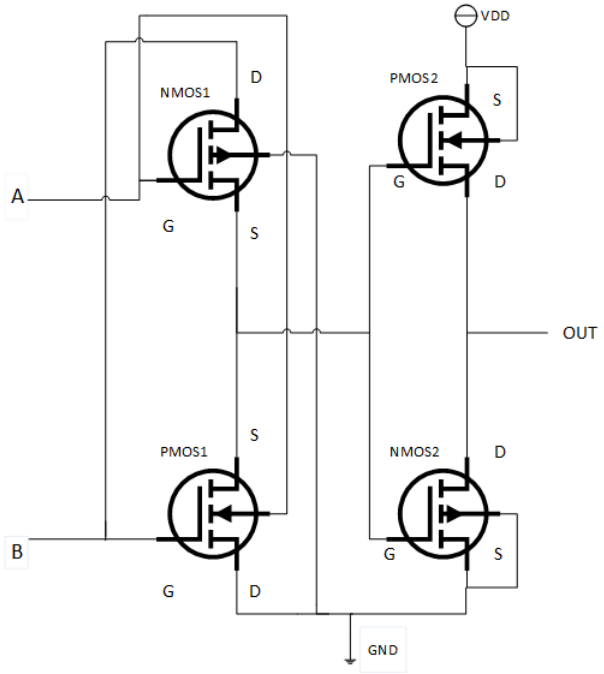

Figure 4.6: Proposed NAND gate

Logic	**Power (micro watts)**	**Delay (ns)**	**Number of transistors**
Proposed	0.88	3.007	2
CMOS ($2n$) [11]	4.42	2.959	6

Table 4.2: Comparison between the proposed gate and the conventional design

The proposed NAND gate is designed and simulated in the TSMC 180nm technology, and its transient response is shown in Fig. 4.7.

The proposed NAND is being compared with the conventional gate design for its delay and power consumed. For comparison purposes, the conventional AND gate is also implemented and simulated. The transistor-level design of the conventional gate is shown in Fig. 4.9. Table 4.2 presents the comparison between the proposed and conventional design $2n$ logic [11].

The comparison in Table 4.2 depicts that the novel AND gate design has less power consumption and area when compared with the conventional AND gate design.

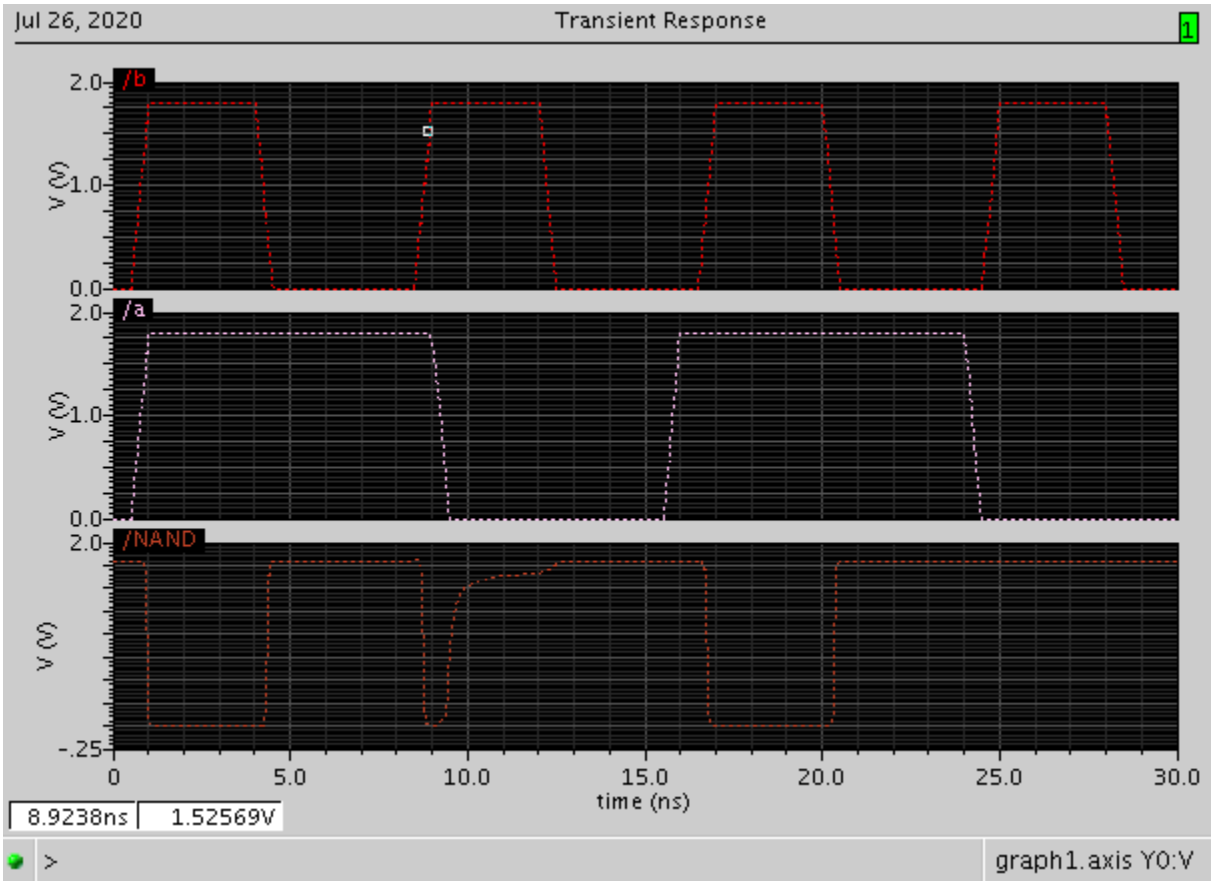

Figure 4.7: NAND gate transient analysis

This approach in creating combinational logic also creates a methodology for the usage of n number of transistors for n number of inputs. This is achieved by adding an extra $NMOS$ in a cascade fashion. The SR-Latch is designed and implemented in Cadence, and its transient response is presented in Fig. 4.8. Here S bar and R bar is the input while Q and Q bar is its output.

Each output of the SR-latch is given to a coincident circuit which generates output in the form of a loop like a hysteresis.

This is introduced to increase the bit rate stability of the entire model. The circuit is then made into P-cell so that it could be made into a complete custom layout model. Here we induced a few layout randomnesses as an additional form so it could produce

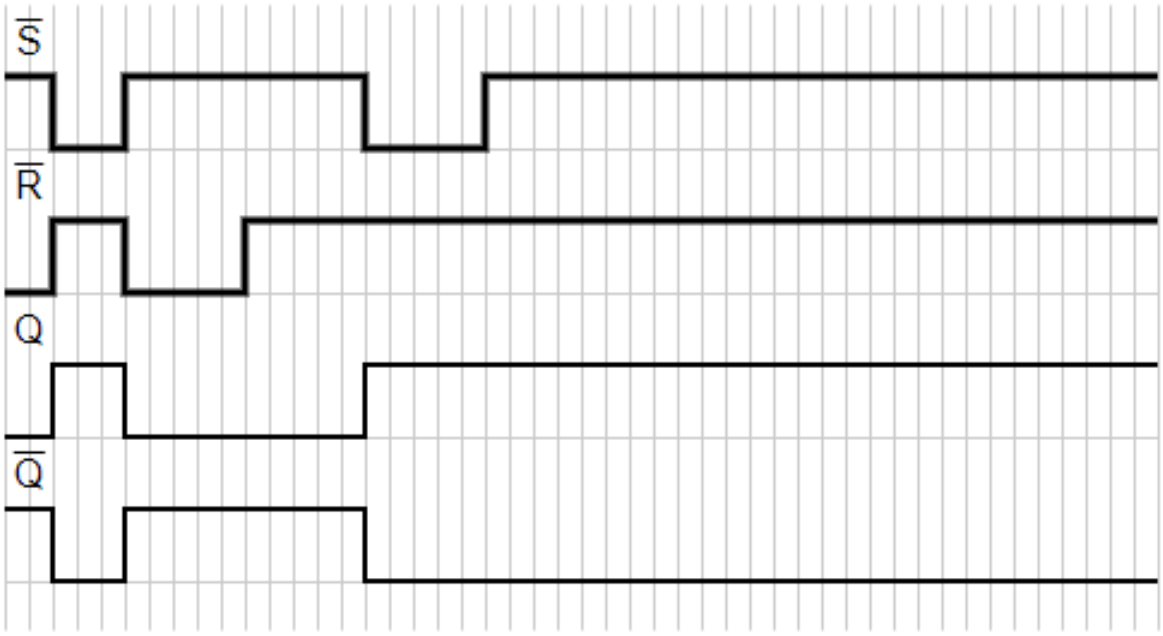

Figure 4.8: SR latch transient analysis

more reliable outputs.

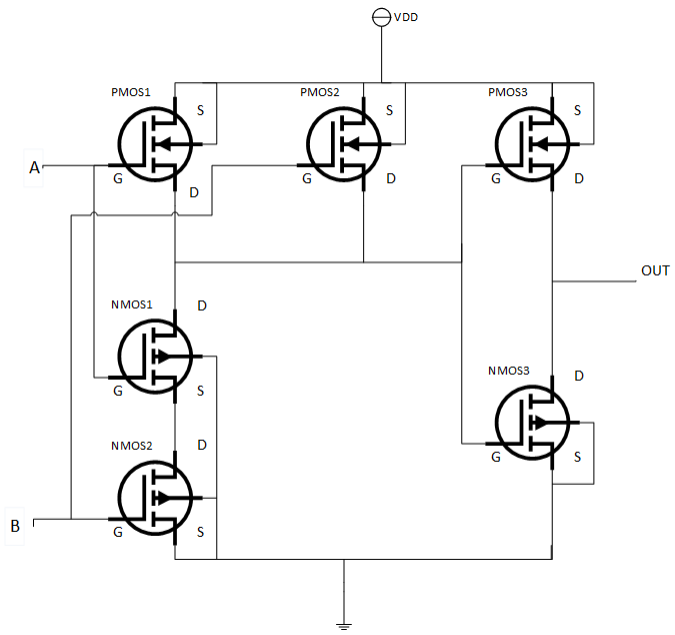

Figure 4.9: AND gate (conventional)[11]

4.4 4-Input Coincident Circuit

The coincident circuit produces an output which is like a hysteresis loop. The circuit is a four-way input that converts the output to a single voltage level output. This way the output is randomized. Fig 4.11 represents the gate level structure of this block.

The reason for the coincident circuit's addition is to improve the Bit Error Rate (BER), which is caused by the voltage fluctuations. This block was designed in the TSMC 180nm technology, and a custom layout was made for this model for further analysis.

As a part of testing, parametric simulations were made under various conditions. This work is also proposing a solution to induce layout variations to create unique variations in the circuit. Here $A, B, C, andD$ are inputs while Y is the output. The design for the circuit is formed using a Boolean expression as follows:

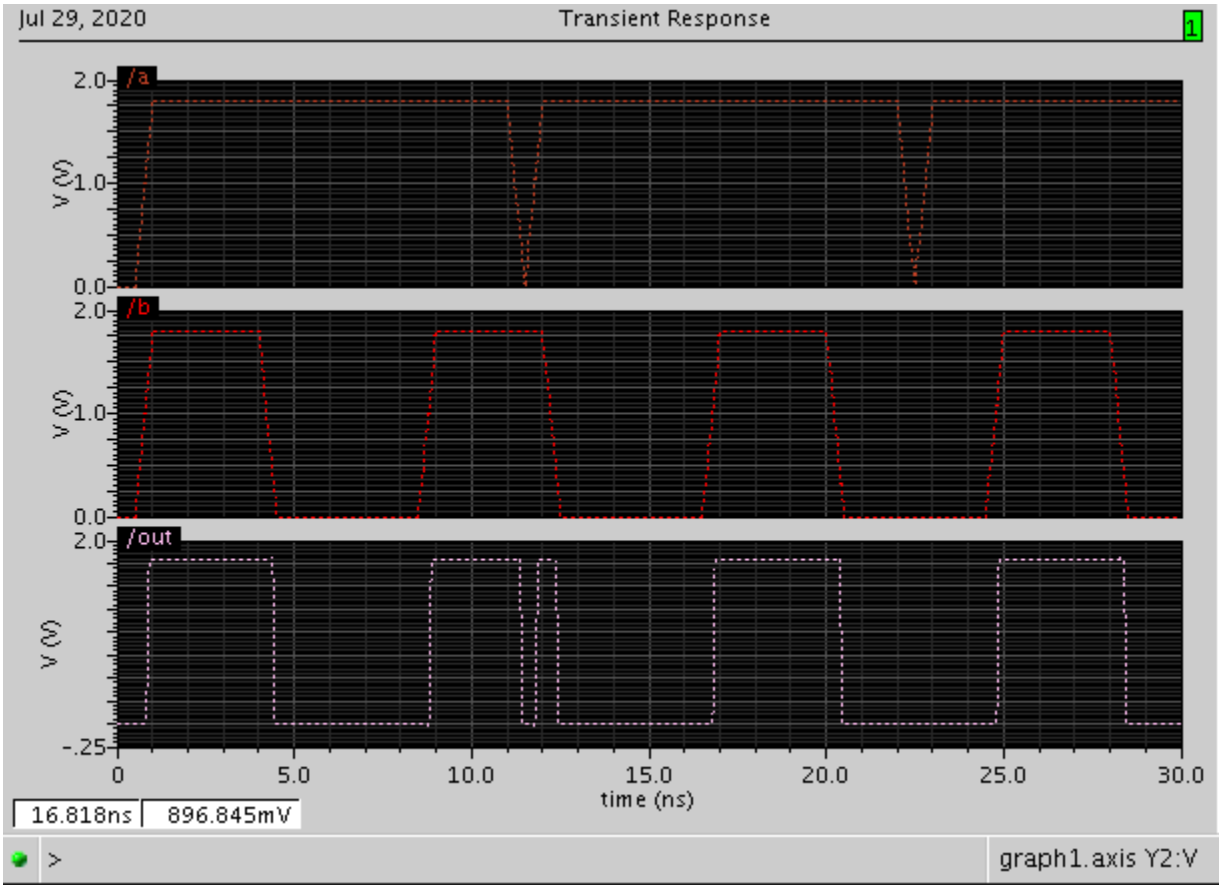

Figure 4.10: AND gate (conventional)transient analysis [11]

$$Y = ABCDVy(AvBvCvD)$$

A total of sixteen different combinations could be formed using this model. The circuit works in such a fashion that few results show opposite behavior with few input results, and it behaves like a magnetic loop similar structure.

4.4.1 Benefits from 4-Bit Coincident Gate

The addition of the Muller C-element (coincident circuit)[**?**]

The circuit behaves like a hysteresis circuit and creates randomness. During the fabrication process, manufacturing causes a mismatch in the circuit. This in turn creates small changes in the transistor dimensions that affect the response bits. This creates higher randomness in the PUF, which is not following a known mathematical model, hence making the PUF stronger against attacks. This model was designed for a 4-bit configuration and then tested successfully over the Cadence Virtuoso using the ADE tool. The transistor-level of the circuit is shown in Fig. 4.11

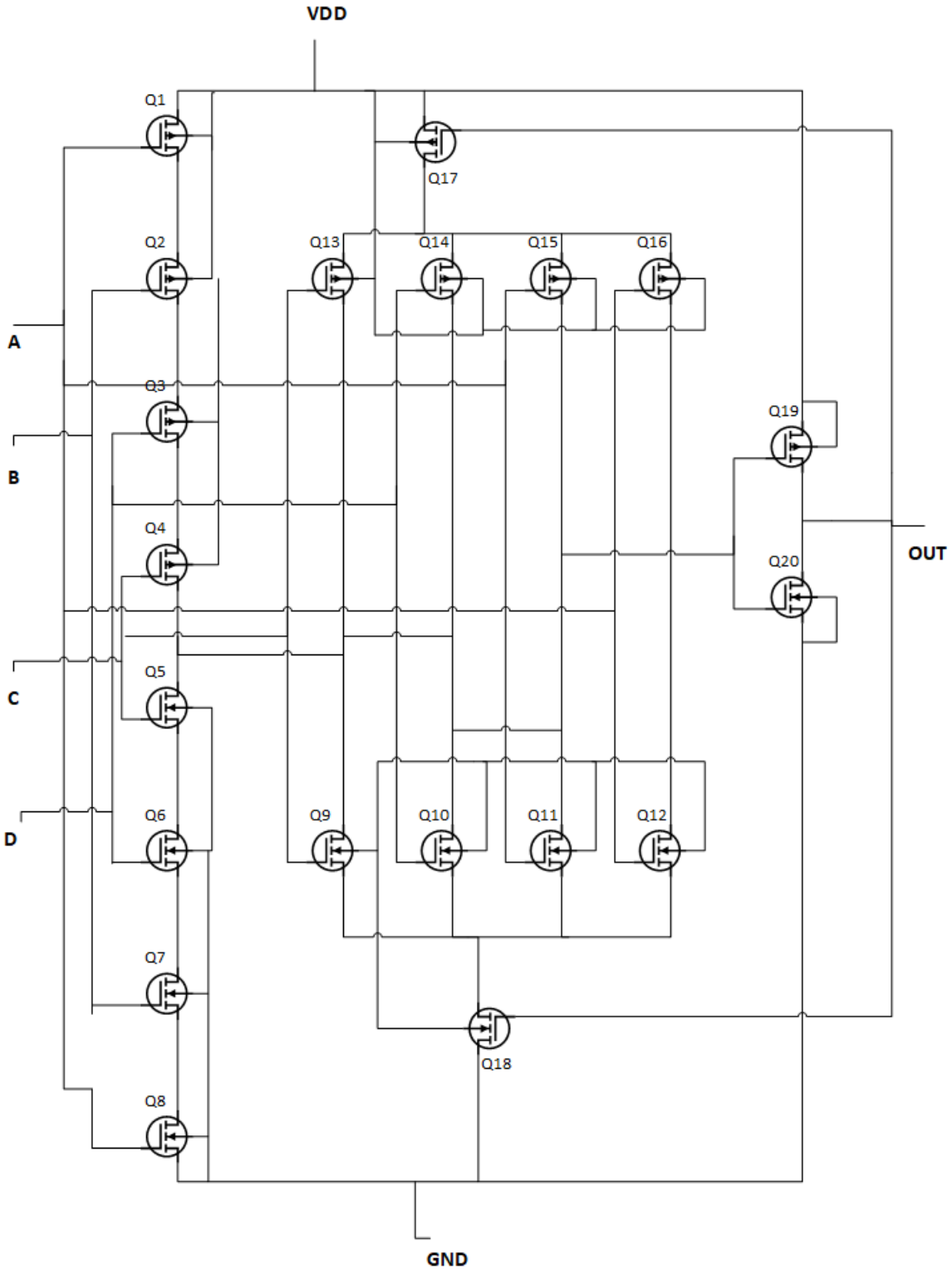

Figure 4.11: 4-bit coincident circuit

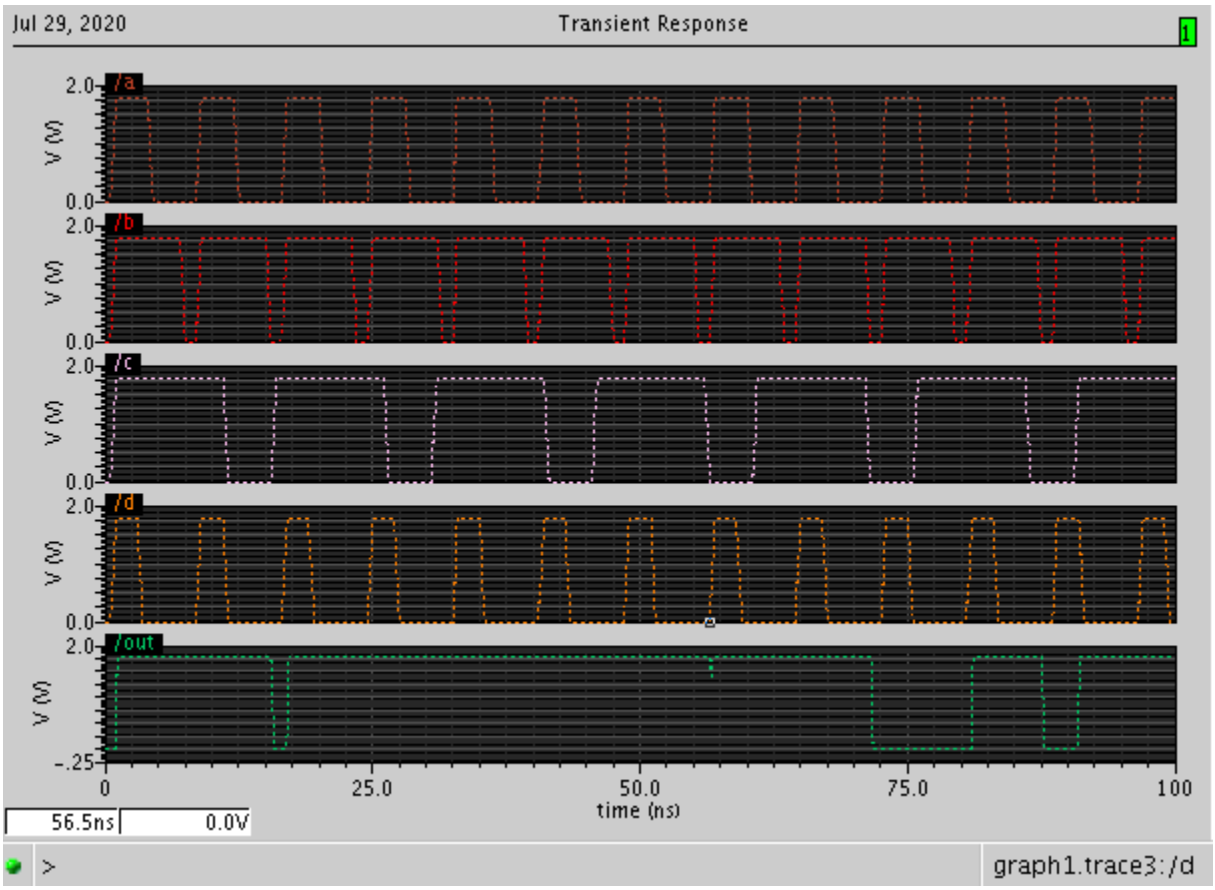

Figure 4.12: 4-bit coincident circuit transient analysis

Chapter 5

Conclusion

This chapter concludes the thesis work conducted and discuss its future work and implementation.

5.1 Summary of contribution

This thesis is an implementation of a Mixed-signal PUF model which focuses on low power device primarily applications for the IoT and sensor network applications.

In this thesis work, 8-bit, 16-bit, 32-bit, and 64-bit PUFs, using P-cell blocks were implemented. PUFs were evaluated for their uniqueness, reliability, area, and power consumption. Here we have used cadence IC 5.1.4 Virtuoso to evaluate its schematics, layout, and RC extraction. RC extraction here was used to analyze Monte Carlo analysis (process variations) with temperature 1 to 125 degrees Celsius was conducted for predicting the uniqueness and reliability of the cell. Spectre S spice models from the TSMC were used for simulations.

The performance of the models is studied using four combinations of cells made using basic P-cell blocks, namely 8-bit, 16-bit, 32-bit, and 64-bit. The uniqueness is estimated to be 50.55%, 49.68%, 49.96%, and 48.68%, respectively, for 8-bit, 16-bit, 32-bit, and 64-bit. The device's reliability was calculated using Intra-hamming distance, which was calculated to be approximately 99.504%, 99.337%, 99.012%, and 99.788% respectively for 8-bit, 16-bit, 32-bit, and 64-bit. The thesis also compares a few existing models. The energy consumption of the proposed model is estimated to be 0.1130 fJ/bit which is comparatively lesser than the models compared.

In addition, we have proposed a AND gate structure, which reduces power consumption to a great extent from the actual CMOS 2n logic. The results obtained in this thesis are well obtained using Monte Carlo analysis. This model could be implemented in applications such as authentication and secret key generation for low power applications like IoT. One could fabricate the IC and test the units over multiple environmental conditions to find out its range of performance in more accurate real-time.

All performance parameters proportionality depends on layout factors such as electromigration, IR, and Antenna effects when reproduced, which in turn depends upon the parameters such as uniqueness, reliability, and energy consumption.

5.2 Conclusion

This research aimed to present a low power PUF unit that could be widely used in IoT devices. The design is incorporated with standard cell-based design flow; this methodology could be used to develop larger PUF units with basic standard cell blocks (P-cell) when compared with conventional design techniques. The standard cell approach provides the designer the ability to submerge the PUF core on to the basic cells, which allows natural obfuscation.

Test-design using cadence virtuoso in 180nm has achieved a very low power consumption ($0.01124 microwatts@1GHz$), this is basically by the introduction of novel SR-latch model. Based on quantitative and qualitative analysis, the research has come to the conclusion that the designed PUF unit consumes the lowest power when compared with similar models, as shown in comparison studies.

As a future extension for research, various combinations could be tired to reduce hardware complexities to even reduce power consumption and increase performance. Introduction to the control unit could even improve the reliability of the circuit to be greater extend.

Finally, the proposed PUF using a standard cell approach reduces the designer's effort in building the design from scratch. The time scale is reduced down to days instead of weeks and months for a conventional analog and digital type PUF model. Considering the factors such as low energy consumption, low design effort, and high-quality output, this design is ideal for unique signature/ secure key generation systems in hardware secure low-cost low-power IoT devices.

5.3 Future work

The planned work for the extended implementation of the same is shown in the flow chart below. The layout designed here could generate a standard cell library in a Verilog environment and then be used to implement the desired configuration. Once the design model is met, it can be used to test over in FPGA in real-time.

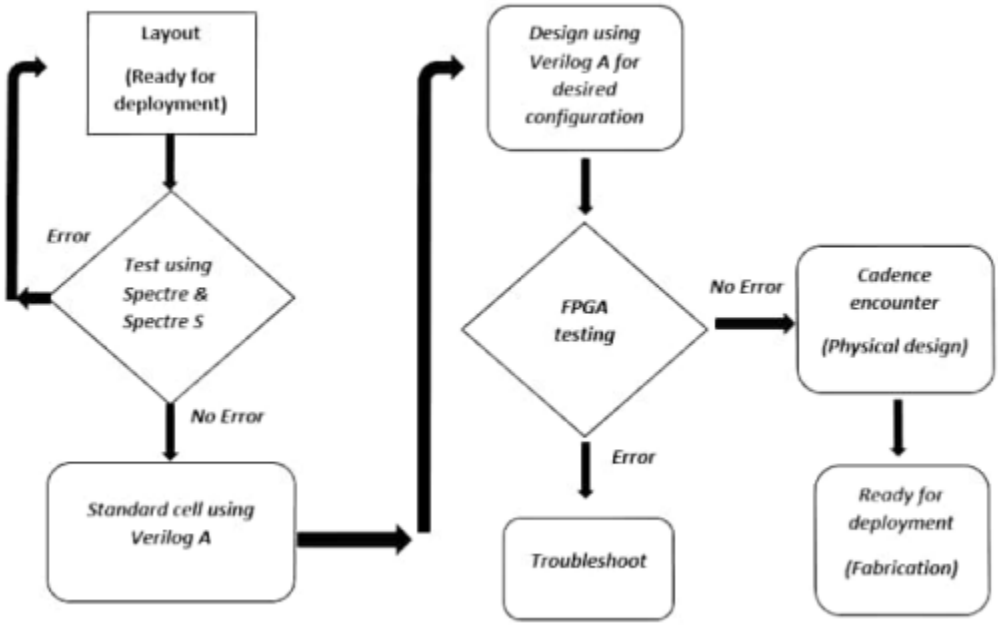

Figure 5.1: Future work

Testing can be used over different areas of FPGA to find out the performance.

Then the design is then sent out to the cadence encounter platform for the final layout, which includes physical design for the chip (power, clock synthesis, etc.). Once the final layout is completed, the design is then sent for fabrication.

References

[1] Z. Paral and S. Devadas, "Reliable and efficient puf-based key generation using pattern matching," in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 2011, pp. 128–133.

[2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[3] J. H. Anderson, "A puf design for secure fpga-based embedded systems," in *2010 15th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2010, pp. 1–6.

[4] V. Sehwag and T. Saha, "Tv-puf: a fast lightweight analog physical unclonable function," in *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*. IEEE, 2016, pp. 182–186.

[5] B. Wilamowski, E. Ferre-Pikal, and O. Kaynak, "Low power, current mode cmos circuits for synthesis of arbitrary nonlinear functions," in *9th NASA Symposium on VLSI Design*, 2000, pp. 7–3.

[6] Q. Guo, J. Ye, Y. Gong, Y. Hu, and X. Li, "Efficient attack on non-linear current mirror puf with genetic algorithm," in *2016 IEEE 25th Asian Test Symposium (ATS)*. IEEE, 2016, pp. 49–54.

[7] S. Taneja, A. B. Alvarez, and M. Alioto, "Fully synthesizable puf featuring hysteresis and temperature compensation for 3.2% native ber and 1.02 fj/b in 40 nm," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 10, pp. 2828–2839, 2018.

[8] A. Ardakani, S. B. Shokouhi, and A. Reyhani-Masoleh, "Improving performance of fpga-based sr-latch puf using transient effect ring oscillator and programmable delay lines," *Integration*, vol. 62, pp. 371–381, 2018.

[9] "Technology - intrinsic id — iot security," https://www.intrinsic-id.com/sram-puf/, (Accessed on 07/16/2020).

[10] L. T. Clark, S. B. Medapuram, D. K. Kadiyala, and J. Brunhaver, "Physically unclonable functions using foundry sram cells," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 3, pp. 955–966, 2018.

[11] A. Morgenshtein, A. Fish, and I. A. Wagner, "Gate-diffusion input (gdi)-a technique for low power design of digital circuits: analysis and characterization," in *2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353)*, vol. 1. IEEE, 2002, pp. I–I.

[12] A. J. Bhavnagarwala, X. Tang, and J. D. Meindl, "The impact of intrinsic device fluctuations on cmos sram cell stability," *IEEE journal of Solid-state circuits*, vol. 36, no. 4, pp. 658–665, 2001.

[13] "Gartner," https://www.gartner.com/en, (Accessed on 06/19/2020).

[14] "Cyber threat intelligence – cyber security report — sonicwall - sonicwall," https://www.sonicwall.com/2020-cyber-threat-report/, (Accessed on 04/05/2020).

[15] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[16] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[17] I. A. B. Adames, J. Das, and S. Bhanja, "Survey of emerging technology based physical unclonable funtions," in *2016 International Great Lakes Symposium on VLSI (GLSVLSI)*. IEEE, 2016, pp. 317–322.

[18] A. Maiti, I. Kim, and P. Schaumont, "A robust physical unclonable function with enhanced challenge-response set," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 333–345, 2011.

[19] S. U. Hussain, S. Yellapantula, M. Majzoobi, and F. Koushanfar, "Bist-puf: Online, hardware-based evaluation of physically unclonable circuit identifiers," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2014, pp. 162–169.

[20] "Nptel open online course (noc) — indian institute of technology madras," https://www.iitm.ac.in/content/nptel-open-online-course-noc-0, (Accessed on 04/05/2020).

[21] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded systems design with FPGAs*. Springer, 2013, pp. 245–267.

[22] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A puf taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011303, 2019.

[23] F. Armknecht, R. Maes, A.-R. Sadeghi, F.-X. Standaert, and C. Wachsmann, "A formalization of the security features of physical functions," in *2011 IEEE Symposium on Security and Privacy*. IEEE, 2011, pp. 397–412.

[24] K. Lofstrom, W. R. Daasch, and D. Taylor, "Ic identification circuit using device mismatch," in *2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No. 00CH37056)*. IEEE, 2000, pp. 372–373.

[25] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2007, pp. 63–80.

[26] C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, "Physically uncloneable functions in the universal composition framework," in *Annual Cryptology Conference*. Springer, 2011, pp. 51–70.

[27] U. Rührmair and D. E. Holcomb, "Pufs at a glance," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2014, pp. 1–6.

[28] Y. Gao, H. Ma, S. F. Al-Sarawi, D. Abbott, and D. C. Ranasinghe, "Puf-fsm: A controlled strong puf," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 5, pp. 1104–1108, 2017.

[29] S. Thomas *et al.*, "A detailed review on physical unclonable function circuits for hardware security," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2018, pp. 609–612.

[30] K. Fruhashi, M. Shiozaki, A. Fukushima, T. Murayama, and T. Fujino, "The arbiter-puf with high uniqueness utilizing novel arbiter circuit with delay-time measurement," in *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*. IEEE, 2011, pp. 2325–2328.

[31] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525)*. IEEE, 2004, pp. 176–179.

[32] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[33] B. Gassend, D. Lim, D. Clarke, M. Van Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurrency and Computation: Practice and Experience*, vol. 16, no. 11, pp. 1077–1098, 2004.

[34] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237–249.

[35] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable pufs," *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 2, no. 1, pp. 1–33, 2009.

[36] N. Bochard, F. Bernard, V. Fischer, and B. Valtchanov, "True-randomness and pseudo-randomness in ring oscillator-based true random number generators," *International Journal of Reconfigurable Computing*, vol. 2010, 2010.

[37] P. Bayon, L. Bossuet, A. Aubert, and V. Fischer, "Em radiation analysis on true random number generators: Frequency and localization retrieval method," 2013.

[38] S. Gören, O. Ozkurt, A. Yildiz, H. F. Ugurdag, R. S. Chakraborty, and D. Mukhopadhyay, "Partial bitstream protection for low-cost fpgas with physical unclonable function, obfuscation, and dynamic partial self reconfiguration," *Computers & Electrical Engineering*, vol. 39, no. 2, pp. 386–397, 2013.

[39] K. Shimizu, D. Suzuki, and T. Kasuya, "Glitch puf: extracting information from usually unwanted glitches," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 95, no. 1, pp. 223–233, 2012.

[40] X. Zhao, P. Gan, Q. Zhao, D. Liang, Y. Cao, X. Pan, and A. Bermak, "A 124 fj/bit cascode current mirror array based puf with 1.50% native unstable bit ratio," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 9, pp. 3494–3503, 2019.

[41] H. Hata and S. Ichikawa, "Fpga implementation of metastability-based true random number generator," *IEICE TRANSACTIONS on Information and Systems*, vol. 95, no. 2, pp. 426–436, 2012.

[42] Y. Su, J. Holleman, and B. Otis, "A 1.6 pj/bit 96% stable chip-id generating circuit using process variations," in *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*. IEEE, 2007, pp. 406–611.

[43] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic pufs from flip-flops on reconfigurable devices," in *3rd Benelux workshop on information and system security (WISSec 2008)*, vol. 17, 2008, p. 2008.

[44] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Springer, 2010, pp. 3–37.

[45] A. Alvarez, W. Zhao, and M. Alioto, "14.3 15fj/b static physically unclonable functions for secure chip identification with¡ 2% native bit instability and 140× inter/intra puf hamming distance separation in 65nm," in *2015 IEEE International Solid-State Circuits Conference-(ISSCC) Digest of Technical Papers*. IEEE, 2015, pp. 1–3.

[46] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *2009 International Conference on Field Programmable Logic and Applications*. IEEE, 2009, pp. 703–707.

[47] "C-element - wikipedia," https://en.wikipedia.org/wiki/C-element, (Accessed on 07/28/2020).

Appendix:IEEE Permission to Reprint

In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of University of Windsor's products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

Vita Auctoris

NAME	:	Harikrishnan Balagopal
BIRTH YEAR	:	1995
BIRTH PLACE	:	India
EDUCATION		
2020	:	**Masters of Applied Science**
		Department of Electrical and Computer Engineering
		University of Windsor, Windsor, Ontario, Canada
2017	:	**Bachelors of Technology**
		Department of Electronics and Communication Engineering
		Jain University, Bangalore, Karnataka, India